PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-189015

(43)Date of publication of application : 10.07.2001

---

(51)Int.Cl. G11B 7/004
G11B 7/24
G11B 19/04
G11B 19/12
G11B 20/10
G11B 20/12
H04L 9/08

---

(21)Application number : 2000-125933 (71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 26.04.2000 (72)Inventor : NAGAI TAKAHIRO
ISHIHARA SHUJI
TAKAGI YUJI
YUMIBA TAKASHI
SHOJI MAMORU
OSHIMA MITSUAKI
OHARA SHUNJI
ITOU MOTOYUKI
ISHIDA TAKASHI
NAKAMURA ATSUSHI
SHIYABANA MASAJI
NAKADA KOHEI

---

(30)Priority
Priority number : 11122104
11128197
11299635
Priority date : 28.04.1999
10.05.1999
21.10.1999
Priority country : JP
JP
JP

---

(54) OPTICAL DISK, OPTICAL DISK RECORDER, OPTICAL DISK REPRODUCER, OPTICAL DISK RECORDING/REPRODUCING DEVICE, OPTICAL DISK RECORDING/REPRODUCING METHOD, OPTICAL DISK RECORDING METHOD, OPTICAL DISK REPRODUCING METHOD, OPTICAL DISK DELETING METHOD, AND INFORMATION PROCESSING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent the unauthorized digital copy from a recording type optical disk to other recording type optical disks.
SOLUTION: In the recording type optical disk capable of recording data, the data recording/reproducing area for recording and reproducing the data and the disk discriminating information area for reproduction only to record the disk discriminating information for discriminating the optical disk are included. This discriminating information is formed by removing the reflection film on the optical disk to the stripe state. The above disk discriminating information includes disk discriminators intrinsic for each optical disk. Also, the data recording/reproducing area includes the area for recording the data cipered by using the information including the disk discriminating information for discriminating the optical disk as a key.

LEGAL STATUS [Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The optical disk characterized by including the data-logging playback field which records data and is reproduced in the record mold optical disk which can record data, and the disk identification information field only for playbacks which records the disk identification information for identifying the above-mentioned optical disk.

[Claim 2] The above-mentioned disk identification information is an optical disk according to claim 1 characterized by being formed by removing the reflective film on the above-mentioned optical disk in the shape of a stripe.

[Claim 3] The above-mentioned disk identification information is an optical disk according to claim 1 characterized by including a peculiar disk identifier for every optical disk.

[Claim 4] The above-mentioned data-logging playback field is an optical disk according to claim 1 characterized by including the field which records the data enciphered using the information containing the disk identification information for identifying the

above-mentioned optical disk as a key.

[Claim 5] The data by which encryption was carried out [above-mentioned] are an optical disk according to claim 4 characterized by the thing of image data and the music data which it comes out on the other hand at least, and is included for the data of a certain contents.

[Claim 6] The data by which encryption was carried out [above-mentioned] are an optical disk according to claim 4 or 5 characterized by including the descrambling key for solving the code given to the data of contents.

[Claim 7] The data by which encryption was carried out [above-mentioned] are an optical disk according to claim 4 or 5 characterized by including the descrambling key for solving the code given to the data of contents, and the error detecting code for detecting the error of the above-mentioned descrambling key.

[Claim 8] In the record mold optical disk which can record data the above-mentioned optical disk The data-logging playback field which records data and is reproduced is included. The above-mentioned data-logging playback field The optical disk characterized by including the field which records the descrambling key for solving the code given to the data of the contents which are at least one side of the music data enciphered as the enciphered image data, and the data of the above-mentioned contents.

[Claim 9] The data and the above-mentioned descrambling key of the above-mentioned contents are an optical disk according to claim 8 characterized by what was recorded in the same sector.

[Claim 10] The data and the above-mentioned descrambling key of the above-mentioned contents are an optical disk according to claim 8 characterized by what was recorded on a different sector.

[Claim 11] The optical disk according to claim 10 characterized by recording the pointer in which the field where the above-mentioned descrambling key is recorded on the sector on which the above-mentioned contents were recorded is shown.

[Claim 12] The disk identification information field only for playbacks which records the disk identification information for identifying the above-mentioned optical disk in the record mold optical disk which can record data, The data-logging playback field which records the data of the contents containing at least one of the enciphered image data and the enciphered music data, and is reproduced, The optical disk characterized by including the key management information field which records the key information used when reproducing the data of the above-mentioned contents, and the descrambling key enciphered using the above-mentioned disk identification information as a key.

[Claim 13] The record actuation which records data to the data-logging playback field of

the record mold optical disk which can record data, It is the optical disk record regenerative apparatus which controls at least one side of the playback actuation which reproduces data from the above-mentioned data-logging playback field. The above-mentioned optical disk A playback means to reproduce the above-mentioned disk identification information from the above-mentioned disk identification information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, Based on the disk identification information by which playback was carried out [above-mentioned], it judges whether at least one of the above-mentioned record actuation and the above-mentioned playback actuation is performed, and is based on the decision result concerned. The above-mentioned record actuation, The optical disk record regenerative apparatus characterized by having the control means controlled to perform at least one side of the above-mentioned playback actuation.

[Claim 14] In the optical disk recording apparatus which records the data of contents to the record mold optical disk which can record data the above-mentioned optical disk A playback means to reproduce disk identification information from the above-mentioned disk identification information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, The optical disk recording device characterized by having a record means to record the data with which at least the part was enciphered to the above-mentioned optical disk, using as a key the disk identification information by which playback was carried out [above-mentioned].

[Claim 15] The data by which encryption was carried out [above-mentioned] are an optical disk recording device according to claim 14 characterized by including the descrambling key for solving the code given to the data of the above-mentioned contents.

[Claim 16] The data by which encryption was carried out [above-mentioned] are an optical disk recording device according to claim 14 characterized by including the descrambling key for solving the code given to the data of the above-mentioned contents, and the error detecting code for detecting the error of the above-mentioned descrambling key.

[Claim 17] In the optical disk regenerative apparatus which reproduces the data of contents from the record mold optical disk which can record data the above-mentioned optical disk A playback means to reproduce disk identification information from the above-mentioned disk identification information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, The optical disk regenerative apparatus characterized by

having a decryption means to decrypt using as a key the disk identification information by which playback was carried out [above-mentioned] after reproducing the data with which at least the part was enciphered from the above-mentioned optical disk.

[Claim 18] The above-mentioned data by which a decryption is carried out are an optical disk regenerative apparatus according to claim 17 characterized by including the descrambling key for solving the code given to the data of the above-mentioned contents.

[Claim 19] The above-mentioned decryption means is an optical disk regenerative apparatus according to claim 17 characterized by detecting the error contained in the above-mentioned descrambling key based on the above-mentioned error detecting code including a descrambling key for the above-mentioned data by which a decryption is carried out to solve the code given to the data of the above-mentioned contents, and the error detecting code for detecting the error of the above-mentioned descrambling key.

[Claim 20] The optical disk recording apparatus characterized by having a record means to record the descrambling key for solving the code given to the data of the enciphered contents, and the data of the above-mentioned contents in the optical disk recording apparatus which records the data of contents to the record mold optical disk which can record data on the above-mentioned optical disk.

[Claim 21] The above-mentioned record means is an optical disk recording device according to claim 20 characterized by what the data of the contents by which encryption was carried out [above-mentioned] are recorded on the 1st predetermined sector, and is recorded on the 2nd sector from which the 1st sector of the above differs the above-mentioned descrambling key.

[Claim 22] The above-mentioned record means is an optical disk recording device according to claim 21 characterized by recording the pointer in which the field in the 2nd sector by which the above-mentioned descrambling key was recorded on the 1st sector on which the data of the contents by which encryption was carried out [above-mentioned] were recorded is shown.

[Claim 23] The optical disk regenerative apparatus characterized by having a playback means to reproduce the descrambling key for solving the code given to the data of the contents enciphered in the optical disk regenerative apparatus which reproduces the data of contents from the record mold optical disk which can record data, and the data of the above-mentioned contents from the above-mentioned optical disk.

[Claim 24] The above-mentioned playback means is an optical disk regenerative apparatus according to claim 23 characterized by reproducing the contents by which encryption was carried out [above-mentioned] from the 1st sector of the above-mentioned optical disk, and reproducing from the 2nd sector from which the 1st

sector of the above differs the above-mentioned descrambling key.

[Claim 25] The above-mentioned playback means is an optical disk regenerative apparatus according to claim 24 characterized by reproducing the pointer in which the field in the 2nd sector by which the above-mentioned descrambling key is reproduced is shown from the 1st sector on which the data of the contents by which encryption was carried out [above-mentioned] were recorded.

[Claim 26] To the key management information field of the record mold optical disk which can record data An acquisition means to be the optical disk recording apparatus which assigns and records the information on a descrambling key required in order to encipher the data of contents, and to acquire the information about a descrambling key required for the data of contents which should be recorded, The information on the descrambling key by which reproduced the information on the descrambling key recorded on the above-mentioned key management information field, and playback was carried out [above-mentioned], The optical disk recording device characterized by having the allocation means which assigns the field which records the descrambling key which should be recorded in the above-mentioned key management information field based on the information about the descrambling key by which acquisition was carried out [above-mentioned].

[Claim 27] To the key management information field of the record mold optical disk which can record data An acquisition means to be the optical disk recording apparatus which records the information on a descrambling key required in order to encipher the data of contents, and to acquire a descrambling key required in order to reproduce the data of contents, The information on the descrambling key recorded on the above-mentioned key management information field is reproduced. The optical disk recording device characterized by having a record means to record arranging the descrambling key by which acquisition was carried out [above-mentioned] in the above-mentioned key management information field based on the information on the descrambling key by which playback was carried out [above-mentioned].

[Claim 28] In the optical disk recording apparatus which records the data of contents to the record mold optical disk which can record data the above-mentioned optical disk A playback means to reproduce disk identification information from the above-mentioned disk identification information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, A decision means to judge whether the data of contents are recordable on the above-mentioned optical disk based on the disk identification information by which playback was carried out [above-mentioned], When it is judged that the data of the

above-mentioned contents are recordable on the above-mentioned optical disk The allocation means which assigns the field for recording a descrambling key required in order to encipher the data of the above-mentioned contents in the key management information field in the above-mentioned optical disk, The optical disk recording device characterized by having a record means to record the key index which shows the field which records the descrambling key of the data of contents which should be recorded on the same sector as the sector on which the data of the above-mentioned contents which should carry out record were recorded.

[Claim 29] It is the optical disk regenerative apparatus which reproduces a descrambling key from the key management information field of the record mold optical disk which can record data. The above-mentioned optical disk The 1st playback means which reproduces the data of the above-mentioned key management information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, A decision means to judge whether the data of the above-mentioned sector field are scrambled based on the data of the sector field in the key management information field by which playback was carried out [above-mentioned], When it is judged that the data of the above-mentioned sector field are scrambled The key index currently recorded in the same sector field as the sector field where the data of the above-mentioned sector field were recorded is reproduced. The 2nd playback means which reproduces a descrambling key from the descrambling key area shown with the key index by which playback was carried out [above-mentioned], The 3rd playback means which reproduces disk identification information from the above-mentioned disk identification information field, The optical disk regenerative apparatus characterized by having a decryption means to reproduce by decrypting the enciphered descrambling key by which playback was carried out [above-mentioned], using as a key the disk identification information by which playback was carried out [above-mentioned].

[Claim 30] It is the optical disk regenerative apparatus according to claim 29 carry out whether the descrambling key by which the decryption was carried out [above-mentioned] is reproduced based on the above-mentioned decision result, and that error detecting code is given to the descrambling key by which the decryption was carried out [above-mentioned], the above-mentioned decryption means judges the existence of the error in the descrambling key by which the decryption was carried out [above-mentioned] based on the error detecting code given to the descrambling key by which the decryption was carried out [above-mentioned], and it judges as the description.

[Claim 31] The record actuation which records data to the data-logging playback field of the record mold optical disk which can record data, It is the optical disk record playback approach which controls at least one side of the playback actuation which reproduces data from the above-mentioned data-logging playback field. The above-mentioned optical disk The step which reproduces the above-mentioned disk identification information from the above-mentioned disk identification information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, Based on the disk identification information by which playback was carried out [above-mentioned], it judges whether at least one of the above-mentioned record actuation and the above-mentioned playback actuation is performed, and is based on the decision result concerned. The above-mentioned record actuation, The optical disk record playback approach characterized by including the step controlled to perform at least one side of the above-mentioned playback actuation.

[Claim 32] In the optical disk record approach which records the data of contents to the record mold optical disk which can record data the above-mentioned optical disk The step which reproduces disk identification information from the above-mentioned disk identification information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, The optical disk record approach characterized by including the step which records the data with which at least the part was enciphered to the above-mentioned optical disk, using as a key the disk identification information by which playback was carried out [above-mentioned].

[Claim 33] In the optical disk playback approach which reproduces the data of contents from the record mold optical disk which can record data the above-mentioned optical disk The step which reproduces disk identification information from the above-mentioned disk identification information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, The optical disk playback approach characterized by including the step decrypted using as a key the disk identification information by which playback was carried out [above-mentioned] after reproducing the data with which at least the part was enciphered from the above-mentioned optical disk.

[Claim 34] The optical disk record approach characterized by including the step which records the descrambling key for solving the code given to the data of the enciphered contents, and the data of the above-mentioned contents in the optical disk record approach which records the data of contents to the record mold optical disk which can

record data on the above-mentioned optical disk.

[Claim 35] The optical disk playback approach characterized by including the step which reproduces the descrambling key for solving the code given to the data of the contents enciphered in the optical disk playback approach which reproduces the data of contents from the record mold optical disk which can record data, and the data of the above-mentioned contents from the above-mentioned optical disk.

[Claim 36] To the key management information field of the record mold optical disk which can record data The step which acquires the information about a descrambling key required for the data of contents which are the optical disk record approach which assigns and records the information on a descrambling key required in order to encipher the data of contents, and should be recorded, The information on the descrambling key by which reproduced the information on the descrambling key recorded on the above-mentioned key management information field, and playback was carried out [above-mentioned], The optical disk record approach characterized by including the step which assigns the field which records the descrambling key which should be recorded in the above-mentioned key management information field based on the information about the descrambling key by which acquisition was carried out [above-mentioned].

[Claim 37] To the key management information field of the record mold optical disk which can record data The step which is the optical disk record approach which records the information on a descrambling key required in order to encipher the data of contents, and acquires a descrambling key required in order to reproduce the data of contents, The information on the descrambling key recorded on the above-mentioned key management information field is reproduced. The optical disk record approach characterized by including the step recorded as arranging the descrambling key by which acquisition was carried out [above-mentioned] in the above-mentioned key management information field based on the information on the descrambling key by which playback was carried out [above-mentioned].

[Claim 38] In the optical disk record approach which records the data of contents to the record mold optical disk which can record data the above-mentioned optical disk The step which reproduces disk identification information from the above-mentioned disk identification information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, The step which judges whether the data of contents are recordable on the above-mentioned optical disk based on the disk identification information by which playback was carried out [above-mentioned], When it is judged that the data of the

above-mentioned contents are recordable on the above-mentioned optical disk The step which assigns the field for recording a descrambling key required in order to encipher the data of the above-mentioned contents in the key management information field in the above-mentioned optical disk, The optical disk record approach characterized by including the step which records the key index which shows the field which records the descrambling key of the data of contents which should be recorded on the same sector as the sector on which the data of the above-mentioned contents which should carry out record were recorded.

[Claim 39] It is the optical disk playback approach which reproduces a descrambling key from the key management information field of the record mold optical disk which can record data. The above-mentioned optical disk The step which reproduces the data of the above-mentioned key management information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, The step which judges whether the data of the above-mentioned sector field are scrambled based on the data of the sector field in the key management information field by which playback was carried out [above-mentioned], When it is judged that the data of the above-mentioned sector field are scrambled The key index currently recorded in the same sector field as the sector field where the data of the above-mentioned sector field were recorded is reproduced. The step which reproduces a descrambling key from the descrambling key area shown with the key index by which playback was carried out [above-mentioned], The optical disk playback approach characterized by including the step which reproduces disk identification information from the above-mentioned disk identification information field, and the step reproduced by decrypting the enciphered descrambling key by which playback was carried out [above-mentioned], using as a key the disk identification information by which playback was carried out [above-mentioned].

[Claim 40] The optical disk characterized by including the 1st information field which records the 1st disk information, the 2nd information field which records the 2nd disk information for identifying each optical disk, and the user data area which records information data by irradiating a light beam to the field concerned in the record mold optical disk which can record data.

[Claim 41] The 2nd disk information of the above is an optical disk according to claim 40 characterized by what was recorded by being a long configuration and removing radially the record film in the information field of the above 2nd selectively in two or more fields.

[Claim 42] The information field of the above 2nd is an optical disk according to claim 40 or 41 characterized by having been arranged in the information field of the above 1st.

[Claim 43] The information field of the above 2nd is an optical disk according to claim 40 or 41 characterized by having been arranged at the inner circumference side of the information field of the above 1st.

[Claim 44] The information field of the above 2nd is an optical disk according to claim 40 or 41 characterized by having been arranged over another field located in an inner circumference side rather than some fields in the information field of the above 1st, and the information field of the above 1st.

[Claim 45] The 1st disk information of the above is claim 40 characterized by what was recorded in the form of the very small concavo-convex pit thru/or the optical disk of one of 44 publications.

[Claim 46] In the record mold optical disk which can record data the above-mentioned optical disk It has the sector structure equipped with two or more sectors. Each above-mentioned sector A sector header field and the Maine data area which records the enciphered data are included. The above-mentioned sector header field The size of the above-mentioned decode key information field is an optical disk characterized by being smaller than the size of each above-mentioned decode key including the decode key information field which records at least one decode key which is the need in order to decrypt the data by which encryption was carried out [above-mentioned].

[Claim 47] It is the optical disk according to claim 46 which each above-mentioned decode key is divided into two or more division decode keys which have predetermined size, and is characterized by recording two or more above-mentioned division decode keys on each decode key information field of two or more continuous sectors.

[Claim 48] The number of partitions of the above-mentioned decode key is an optical disk according to claim 47 characterized by being the divisor of the number of sectors contained in the error correcting code (ECC) block which are two or more sectors required for an error correction.

[Claim 49] The index which shows the record location in the above-mentioned decode key table of a decode key required in order to record each above-mentioned decode key on the decode key table which has two or more decode keys and to decrypt the data by which encryption was carried out [above-mentioned] is an optical disk according to claim 46 characterized by what was recorded on the decode key information field of the above-mentioned sector.

[Claim 50] The optical disk according to claim 49 with which the decode key condition field which recorded the decode key condition over each decode key field of the above-mentioned decode key table was recorded as information showing the record condition of the above-mentioned decode key table.

[Claim 51] The above-mentioned decode key table is an optical disk according to claim 49 characterized by what was recorded over two or more different error correcting code (ECC) blocks.

[Claim 52] Each above-mentioned decode key is an optical disk according to claim 499 characterized by what was managed and recorded in one [at least] unit of the file unit managed in a file management field, and the extent units which consist of two or more sectors which continue on an optical disk.

[Claim 53] In the record mold optical disk which can record data the above-mentioned optical disk The Maine data area which records data is included. The above-mentioned Maine data area The non-enciphering field which records data in the state of un-enciphering, and the encryption field which records data in the state of encryption are included. The above-mentioned non-enciphering field The data of the above-mentioned encryption field are an optical disk characterized by being enciphered using the decode key changed using the above-mentioned decode key translation data including the decode key translation data used for conversion of the decode key for decrypting data.

[Claim 54] The control information record sector on which the above-mentioned Maine data area records the control information used for playback control of data in the state of un-enciphering, The data-logging sector which records data in the state of encryption is included. The above-mentioned control information record sector The data of the above-mentioned data-logging sector are an optical disk according to claim 53 characterized by being enciphered using the decode key changed using the above-mentioned decode key translation data including the decode key translation data used for conversion of the above-mentioned decode key.

[Claim 55] The non-enciphering field where the above-mentioned data-logging sector records data in the state of un-enciphering, The above-mentioned non-enciphering field contains another decode key translation data including the encryption field which records data in the state of encryption. AV data of the above-mentioned encryption field are an optical disk according to claim 54 characterized by being enciphered using the decode key into which the decode key changed using the above-mentioned decode key translation data was changed using 2nd still more nearly another decode key translation data.

[Claim 56] The above-mentioned decode key translation data is an optical disk according to claim 53 characterized by including copy-of-data control information at least.

[Claim 57] In the optical disk record approach for recording data on the record mold

optical disk which can record data When it is judged that there are a step which judges whether the decode key status recorded on the above-mentioned optical disk is read, and there is any free area of a decode key based on the decode key status by which reading appearance was carried out [above-mentioned], and a free area of the above-mentioned decode key The step which reserves a decode key field and records a decode key, and the step which sets up copyright control information and a decode key index in one [at least] unit of a file unit and the extent units, The step which enciphers data using the above-mentioned decode key, and records the enciphered data on the above-mentioned optical disk in one [at least] unit of a file unit and the extent units, The optical disk record approach characterized by including the step which records the file management information for managing the data recorded on the above-mentioned optical disk on the above-mentioned optical disk.

[Claim 58] In the optical disk playback approach for reproducing data from the record mold optical disk which can record data The step which reproduces and acquires a decode key index from the record section of the data which were recorded per the file unit or extent, and which should be reproduced, The optical disk playback approach characterized by including the step which reproduces and acquires the decode key corresponding to the decode key index by which acquisition was carried out [above-mentioned], and the step which reproduces the data of the file unit enciphered using the above-mentioned decode key, or an extent unit.

[Claim 59] In the optical disk deletion approach for deleting data from the record mold optical disk which can record data The step which reproduces and acquires a decode key index from the record section of the data which were recorded per the file unit or extent, and which should be deleted, The step which corresponds to the decode key index by which acquisition was carried out [above-mentioned], updates the decode key status which shows the record condition of a decode key, and opens a decode key, The optical disk deletion approach characterized by including the step which updates the above-mentioned file management information by deleting the file entry corresponding to the above-mentioned data which should carry out deletion from the file management information for managing the data recorded on the above-mentioned optical disk.

[Claim 60] The data encryption equipment which enciphers data using a cryptographic key, and the optical disk record regenerative apparatus which records a decode key required in order to decrypt the above-mentioned data on a record mold optical disk, and is reproduced, It is the information processing system equipped with the control device connected to the above-mentioned optical disk record regenerative apparatus and the above-mentioned data encryption equipment. The above-mentioned optical disk

record regenerative apparatus The 1st record playback means which records a decode key table on the above-mentioned optical disk, and reproduces a decode key table from the above-mentioned optical disk, Encryption and the decryption means of receiving and decrypting the decode key which enciphered the above-mentioned decode key, transmitted to the above-mentioned control unit and was enciphered from the above-mentioned control unit, The decode key condition table showing the record condition of a decode key in the above-mentioned optical disk is recorded. It has the 2nd record playback means which reproduces a decode key condition table from the above-mentioned optical disk. The above-mentioned data encryption equipment It has an encryption means to encipher the above-mentioned decode key and to transmit to the above-mentioned control unit. The above-mentioned control unit A receiving means to receive the decode key enciphered from the encryption means of the above-mentioned data encryption equipment, The free area of a decode key is searched based on the decode key condition table by which playback was carried out [above-mentioned]. The enciphered decode key by which reception was carried out [above-mentioned] is assigned to the free area by which retrieval was carried out [above-mentioned]. It has an allocation means to transmit the enciphered decode key which was assigned the account of a top to the above-mentioned optical disk record regenerative apparatus. Encryption and the decryption means of the above-mentioned optical disk record regenerative apparatus Information processing system characterized by receiving and decrypting the enciphered decode key which was assigned the account of a top from the allocation means of the above-mentioned control unit.

[Claim 61] The optical disk regenerative apparatus which reproduces the decode key table equipped with two or more decode keys required in order to decrypt data and the above-mentioned data from a record mold optical disk, It is the information processing system equipped with the control device connected to the above-mentioned optical disk regenerative apparatus, and the data decryption equipment which decrypts data using a decode key. The above-mentioned optical disk regenerative apparatus The decode key table by which playback was carried out [above-mentioned] is enciphered as the 1st playback means which reproduces a decode key table from the above-mentioned optical disk. An encryption means to transmit the enciphered decode key table to the above-mentioned control unit, It has the 2nd playback means which reproduces the decode key condition table showing the record condition of two or more decode keys from the above-mentioned optical disk. The above-mentioned control unit A receiving means to receive the decode key table by which encryption was carried out [above-mentioned] from the above-mentioned optical disk regenerative apparatus, It has a retrieval means

to search the enciphered decode key required in order to decrypt the data recorded on the above-mentioned optical disk from the decode key table by which reception was carried out [above-mentioned] based on the decode key condition table by which playback was carried out [above-mentioned], and to transmit to the above-mentioned data decryption means. The above-mentioned data decryption equipment Information processing system characterized by having the 1st decryption means which decrypts the decode key by which encryption was carried out [above-mentioned], and generates a decode key, and the 2nd decryption means which decrypts the enciphered data which were reproduced with the optical disk regenerative apparatus using the decode key by which the decryption was carried out [above-mentioned].

[Claim 62] In the optical disk recording apparatus which records data on the record mold optical disk which can record data the above-mentioned optical disk The data containing the decode key translation data used for conversion of the decode key for decrypting data are recorded on the above-mentioned non-enciphering field in the state of un-enciphering including a non-enciphering field and an encryption field. The optical disk recording device characterized by having a record means to record the data enciphered using the decode key changed using the above-mentioned decode key translation data on the above-mentioned encryption field.

[Claim 63] The above-mentioned optical disk contains a control information record sector and a data-logging sector. The above-mentioned record means The control information used for playback control of the above-mentioned data is recorded on the above-mentioned control information record sector in the state of un-enciphering. The optical disk recording device according to claim 62 characterized by what it changes into the decode key into which the cryptographic key was changed using the decode key translation data contained in the above-mentioned control information, and data are enciphered using the decode key by which conversion was carried out [above-mentioned], and is recorded on the above-mentioned data-logging sector.

[Claim 64] It is the optical disk recording device according to claim 63 carry out the above-mentioned record means recording the data containing another decode key translation data on the non-enciphering field of the above-mentioned data-logging sector in the state of un-enciphering, and changing to the decode key into which a cryptographic key was changed using the decode key translation data contained in the above-mentioned control information, and the decode key translation data according to above, enciphering data using the decode key by which conversion was carried out [above-mentioned], and recording to the above-mentioned data-logging sector as the description.

[Claim 65] In the optical disk regenerative apparatus which reproduces data from the record mold optical disk which can record data the above-mentioned optical disk It changes into the decode key into which the decode key was changed using the decode key translation data recorded on the above-mentioned non-enciphering field including a non-enciphering field and an encryption field. The optical disk regenerative apparatus characterized by having a playback means to decrypt the data recorded on the above-mentioned encryption field using the decode key by which conversion was carried out [above-mentioned], and to reproduce.

[Claim 66] The above-mentioned optical disk contains a control information record sector and a data-logging sector. The above-mentioned playback means The control information used for playback control of the above-mentioned data is reproduced from a control information record sector. The optical disk regenerative apparatus according to claim 65 characterized by decrypting the data which changed into the decode key into which the decode key was changed using the decode key translation data contained in the above-mentioned control information, and were recorded on the above-mentioned data-logging sector using the decode key by which conversion was carried out [above-mentioned], and reproducing.

[Claim 67] The decode key translation data which the above-mentioned playback means reproduces another decode key translation data recorded on the non-enciphering field of the above-mentioned data-logging sector, and is contained in the above-mentioned control information, The optical disk regenerative apparatus according to claim 66 characterized by decrypting the data which changed into the decode key into which the decode key was changed using another decode key translation data by which playback was carried out [above-mentioned], and were recorded on the above-mentioned data-logging sector using the decode key by which conversion was carried out [above-mentioned], and reproducing.

[Claim 68] In the optical disk record approach which records data on the record mold optical disk which can record data the above-mentioned optical disk The data containing the decode key translation data used for conversion of the decode key for decrypting data are recorded on the above-mentioned non-enciphering field in the state of un-enciphering including a non-enciphering field and an encryption field. The optical disk record approach characterized by including the step which records the data enciphered using the decode key changed using the above-mentioned decode key translation data on the above-mentioned encryption field.

[Claim 69] In the optical disk playback approach which reproduces data from the record mold optical disk which can record data the above-mentioned optical disk It changes

into the decode key into which the decode key was changed using the decode key translation data recorded on the above-mentioned non-enciphering field including a non-enciphering field and an encryption field. The optical disk playback approach characterized by including the step which decrypts the data recorded on the above-mentioned encryption field using the decode key by which conversion was carried out [above-mentioned], and is reproduced.

[Claim 70] In the mold optical disk only for playbacks for reproducing the recorded data The data playback field where data were recorded, and the disk identification information field only for playbacks where the disk identification information for identifying the above-mentioned optical disk was recorded are included. The above-mentioned data playback field The optical disk characterized by including the field where the data enciphered using the information containing the disk identification information for identifying the above-mentioned optical disk as a key were recorded.

[Claim 71] In the mold optical disk only for playbacks for reproducing the recorded data the above-mentioned optical disk The data playback field where data were recorded is included. The above-mentioned data playback field The optical disk characterized by including the field where the descrambling key for solving the code given to the data of the contents which are at least one side of the music data enciphered as the enciphered image data, and the data of the above-mentioned contents was recorded.

[Claim 72] In the mold optical disk only for playbacks for reproducing the recorded data The disk identification information field only for playbacks where the disk identification information for identifying the above-mentioned optical disk was recorded, The data playback field where the data of the contents containing at least one of the enciphered image data and the enciphered music data were recorded, The optical disk characterized by including the key management information field where the key information used when reproducing the data of the above-mentioned contents, and the descrambling key enciphered using the above-mentioned disk identification information as a key were recorded.

[Claim 73] In the mold optical disk only for playbacks for reproducing the recorded data the above-mentioned optical disk It has the sector structure equipped with two or more sectors. Each above-mentioned sector A sector header field and the Maine data area where the enciphered data were recorded are included. The above-mentioned sector header field The size of the above-mentioned decode key information field is an optical disk characterized by being smaller than the size of each above-mentioned decode key including the decode key information field where at least one decode key which is the need in order to decrypt the data by which encryption was carried out

[above-mentioned] was recorded.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the optical disk and optical disk recording apparatus which can prevent the unjust digital copy to record media [optical disk / with which data, such as AV data (Audio and Visual Data) containing the image data of a film which has copyright, or musical voice data, are recorded], such as other record mold optical disks, an optical disk regenerative apparatus, an optical disk record regenerative apparatus, the optical disk record playback approach, the optical disk record approach, the optical disk playback approach, the optical disk deletion approach, and information processing system.
[0002]
[Description of the Prior Art] Since the non-contact record and the playback which are excellent in random access nature compared with the conventional tape media, and used the laser beam are possible for an optical disk, it has the description that little degradation by repeat utilization is. Furthermore, the optical disk has the description that the duplicate of a large quantity is cheaply possible, by mastering by the disk manufacturer, and, instead, CD (Compact Disk) is general for the record of the conventional analog recording as a digital audio of the quality of loud sound. Furthermore, it is expected in recent years that DVD (Digital Video Disk or Digital Versatile Disk) with which digital recording of the image data of high quality was carried out is commercialized, and the optical disk as a digital recording medium of AV data will develop further from now on.

[0003] On the other hand, like Music CD, CD-ROM, or DVD-ROM, for example, not only the optical disk only for playbacks with which data are beforehand recorded by the disk manufacturer in the form of PURIPITTO but recent years and a user can record AV data at home, the optical disk of record molds, such as CD-R, CD-RW, MO and MD, and DVD-RAM, is developed, and it is spreading at a world.

[0004] Moreover, also in television broadcasting, the digital method in which many channelization and various services are possible is introduced from the conventional analog form, and such an inclination will spread further from now on. It is expected that it is used for record of AV data which set time shift utilization to which makes program selection, and it views and listens as the target core after accumulating especially a record mold optical disk as a record medium of contents distributed by the digitized broadcast or communication link at the time of distribution.

[0005] Conventionally, the optical disk of the record mold used centering on a computer is used for the purpose of preservation of the data which the user himself created, and did not have the structure which restricts the copy between the optical disks of a record mold. Without paying the charge of writing which should be essentially paid to the author of the AV data when a general user copies the data of the recorded optical disk to other record mold optical disks illegally as it is, if the optical disk of a record mold comes to be used widely, since digital recording is possible, it becomes possible for a duplicate unjust without degradation of tone quality or image quality to come to hand, and it is also becoming the factor which checks the extensive ball of good contents. In MD which carries out digital recording of the music etc., the structure which performs the generation control which restricts a recording rate is introduced, it records on an optical disk with generation-control data, and the generation-control data is restricting the count of a copy.

[0006] Moreover, in order to, prevent the unjust copy of CD-ROM or DVD-ROM for example, the burst cutting field (it is called BCA below Burst Cutting Area;.) which is a postscript field for carrying out overwrite of the bar code to the pit section of an optical disk is prepared, and the approach of recording ID which is different for every disk in BCA at the time of manufacture of an optical disk is proposed in international application of the international disclosure number WO 97/No. 14144. Since a password changes with disks ID according to this approach and the information on Disk ID is missing even if it becomes impossible for one password to decode only the code of the disk of one sheet and contents are copied unjustly, contents are no longer decoded.

[0007] Drawing 39 is the block diagram showing the configuration of the user data area of DVD-ROM of the conventional technique, and the configuration of the optical disk

regenerative apparatus which decodes encryption contents from the data of a user data area. In DVD-ROM, as shown in drawing 39 , it is enciphering to the data of contents recorded on a disk.

[0008] In drawing 39 , the user data area of DVD-ROM consists of a sector header field 3201, a Maine data area 3202, and error detecting code 3203. Here, the sector address 3204 which shows the location of a sector, the copyright control information 3205 on which the copyright control information (for example, a scramble flag, copy control information, etc.) about the data recorded on the Maine data area 3202 is recorded, and the decode key 3206 for decoding, when the code is given to the data of the Maine data area 3202 are recorded on the sector header field 3201. Moreover, AV data which mainly need protection of copyrights are enciphered and recorded on the Maine data area 3202.

[0009] At the time of playback of such a user data area, the decode key 3206 required for playback of encryption contents is first obtained from the sector header field 3201. The acquired decode key 3206 is inputted into the key decoder 3207, and the key decoder 3207 decodes a contents decode key using a predetermined disk key, and outputs the inputted decode key 3206 to a decoder 3208. Subsequently, a decoder 3208 decodes the encryption contents of the Maine data area 3202 using the contents decode key by which decode was carried out [above-mentioned] according to the copyright control information 3205 stored in the sector header field 3201 corresponding to the Maine data area 3202, and obtains the decryption contents which are refreshable data.

[0010] It enables it to prevent an unjust duplicate and creation of a pirate edition in the optical disk by the configuration shown in drawing 39 by constituting from drive equipment of a personal computer etc. so that the field which recorded the decode key 3206 may be read and only the optical disk regenerative apparatus which has the authentication function of normal can do it, although read-out to the Maine data area 3202 is possible.

[0011]

[Problem(s) to be Solved by the Invention] however, by the illegal copy prevention approach using generation-control data, modification (modification of the information on "a copy being improper" from "a 1-time copy is possible" -- ") of generation-control data is indispensable at the time of a copy. On the other hand, it had the trouble that an illegal copy could not fully be prevented, by not adding modification, copying the data on an optical disk with generation-control data, or altering and recording generation-control data by computer etc. Furthermore, in order for the generation-control data beforehand recorded with contents to restrict the count of a copy, even if it paid the charge of writing of normal, the copy to the optical disk of others

[data / which were "not being copied" on an optical disk] was not allowed at all, but had the problem that a user had to wait for supply from a contents feeder. All are depended on the ability of a contents feeder not to fully manage the copy to the record mold optical disk which a user performs.

[0012] By a personal computer's high-performance-izing and connecting them to a network further in recent years, it is highly efficient and decode of a high-speed code with two or more personal computers is performed. In order to raise the reinforcement of a code more to such decode, it is necessary to extend the key length of the key used for a code. However, in a key management method which records a decode key on a sector header which is proposed from the former, only the decode key below the die length (size of a decode key field) decided beforehand was recordable, and in order to raise the reinforcement of a code to the future, there was a trouble that key length could not be lengthened.

[0013] The 1st object of this invention is to offer the optical disk and optical disk recording apparatus which solve the above trouble and can prevent the unjust digital copy which a contents feeder cannot manage, an optical disk regenerative apparatus, an optical disk record regenerative apparatus, the optical disk record playback approach, the optical disk record approach, the optical disk playback approach, the optical disk deletion approach, and information processing system.

[0014] Moreover, the 2nd object of this invention is to offer the optical disk and optical disk recording apparatus which can solve the above trouble and can raise more the dependability of a decode key required in order to decrypt the data which need protection of copyrights, an optical disk regenerative apparatus, an optical disk record regenerative apparatus, the optical disk record playback approach, the optical disk record approach, the optical disk playback approach, the optical disk deletion approach, and information processing system.

[0015] Furthermore, the 3rd object of this invention is to offer the optical disk and optical disk recording apparatus with which code reinforcement can set up the above trouble according to the level of the protection of copyrights of contents solved and recorded, an optical disk regenerative apparatus, an optical disk record regenerative apparatus, the optical disk record playback approach, the optical disk record approach, the optical disk playback approach, the optical disk deletion approach, and information processing system.

[0016]

[Means for Solving the Problem] The optical disk concerning this invention is characterized by including the data-logging playback field which records data and is

reproduced, and the disk identification information field only for playbacks which records the disk identification information for identifying the above-mentioned optical disk in the record mold optical disk which can record data.

[0017] In the above-mentioned optical disk, the above-mentioned disk identification information is preferably formed by removing the reflective film on the above-mentioned optical disk in the shape of a stripe. Moreover, in the above-mentioned optical disk, the above-mentioned disk identification information contains a peculiar disk identifier for every optical disk preferably.

[0018] Moreover, in the above-mentioned optical disk, the above-mentioned data-logging playback field includes the field which records the data enciphered using as a key the information which contains the disk identification information for identifying the above-mentioned optical disk preferably. In the above-mentioned optical disk, preferably, on the other hand, it comes out of image data and the music data at least, and the data by which encryption was carried out [above-mentioned] contain the data of a certain contents. Moreover, in the above-mentioned optical disk, the data by which encryption was carried out [above-mentioned] contain the descrambling key for solving preferably the code given to the data of contents. Furthermore, in the above-mentioned optical disk, the data by which encryption was carried out [above-mentioned] contain the descrambling key for solving preferably the code given to the data of contents, and the error detecting code for detecting the error of the above-mentioned descrambling key.

[0019] In the record mold optical disk with which the optical disk concerning this invention can record data the above-mentioned optical disk The data-logging playback field which records data and is reproduced is included. The above-mentioned data-logging playback field It is characterized by including the field which records the descrambling key for solving the code given to the data of the contents which are at least one side of the music data enciphered as the enciphered image data, and the data of the above-mentioned contents.

[0020] In the above-mentioned optical disk, preferably, the data and the above-mentioned descrambling key of the above-mentioned contents are recorded in the same sector, or the data and the above-mentioned descrambling key of the above-mentioned contents are recorded on a different sector. Moreover, in the above-mentioned optical disk, the pointer in which the field where the above-mentioned descrambling key is preferably recorded on the sector on which the above-mentioned contents were recorded is shown is recorded.

[0021] In the record mold optical disk with which the optical disk concerning this invention can record data The disk identification information field only for playbacks

which records the disk identification information for identifying the above-mentioned optical disk, The data-logging playback field which records the data of the contents containing at least one of the enciphered image data and the enciphered music data, and is reproduced, It is characterized by including the key management information field which records the key information used when reproducing the data of the above-mentioned contents, and the descrambling key enciphered using the above-mentioned disk identification information as a key.

[0022] The record actuation which records data to the data-logging playback field of the record mold optical disk with which the optical disk record regenerative apparatus concerning this invention can record data, It is the optical disk record regenerative apparatus which controls at least one side of the playback actuation which reproduces data from the above-mentioned data-logging playback field. The above-mentioned optical disk A playback means to reproduce the above-mentioned disk identification information from the above-mentioned disk identification information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, Based on the disk identification information by which playback was carried out [above-mentioned], it judges whether at least one of the above-mentioned record actuation and the above-mentioned playback actuation is performed, and is based on the decision result concerned. The above-mentioned record actuation, It is characterized by having the control means controlled to perform at least one side of the above-mentioned playback actuation.

[0023] In the optical disk recording apparatus which records the data of contents to the record mold optical disk with which the optical disk recording apparatus concerning this invention can record data the above-mentioned optical disk A playback means to reproduce disk identification information from the above-mentioned disk identification information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, It is characterized by having a record means to record the data with which at least the part was enciphered to the above-mentioned optical disk, using as a key the disk identification information by which playback was carried out [above-mentioned].

[0024] In the above-mentioned optical disk recording apparatus, the data by which encryption was carried out [above-mentioned] contain the descrambling key for solving preferably the code given to the data of the above-mentioned contents. Moreover, in the above-mentioned optical disk recording apparatus, the data by which encryption was carried out [above-mentioned] contain the descrambling key for solving preferably the

code given to the data of the above-mentioned contents, and the error detecting code for detecting the error of the above-mentioned descrambling key.

[0025] In the optical disk regenerative apparatus which reproduces the data of contents from the record mold optical disk with which the optical disk regenerative apparatus concerning this invention can record data the above-mentioned optical disk A playback means to reproduce disk identification information from the above-mentioned disk identification information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, After reproducing the data with which at least the part was enciphered from the above-mentioned optical disk, it is characterized by having a decryption means to decrypt using as a key the disk identification information by which playback was carried out [above-mentioned].

[0026] In the above-mentioned optical disk regenerative apparatus, the above-mentioned data by which a decryption is carried out contain the descrambling key for solving preferably the code given to the data of the above-mentioned contents. Moreover, in an optical disk regenerative apparatus, the above-mentioned decryption means detects the error contained in the above-mentioned descrambling key based on the above-mentioned error detecting code including a descrambling key for the above-mentioned data by which a decryption is carried out to solve preferably the code given to the data of the above-mentioned contents, and the error detecting code for detecting the error of the above-mentioned descrambling key.

[0027] The optical disk recording apparatus concerning this invention is characterized by having a record means to record the descrambling key for solving the code given to the data of the enciphered contents, and the data of the above-mentioned contents on the above-mentioned optical disk in the optical disk recording apparatus which records the data of contents to the record mold optical disk which can record data.

[0028] In the above-mentioned optical disk recording apparatus, the above-mentioned record means records preferably the data of the contents by which encryption was carried out [above-mentioned] on the 1st predetermined sector, and records the above-mentioned descrambling key on the 2nd different sector from the 1st sector of the above. Moreover, in the above-mentioned optical disk recording apparatus, the above-mentioned record means records the pointer in which the field in the 2nd sector by which the above-mentioned descrambling key was recorded on the 1st sector on which the data of the contents by which encryption was carried out [above-mentioned] were recorded preferably is shown.

[0029] The optical disk regenerative apparatus concerning this invention is

characterized by having a playback means to reproduce the descrambling key for solving the code given to the data of the contents enciphered in the optical disk regenerative apparatus which reproduces the data of contents from the record mold optical disk which can record data, and the data of the above-mentioned contents from the above-mentioned optical disk.

[0030] In the above-mentioned optical disk regenerative apparatus, the above-mentioned playback means reproduces preferably the contents by which encryption was carried out [above-mentioned] from the 1st sector of the above-mentioned optical disk, and reproduces the above-mentioned descrambling key from the 2nd different sector from the 1st sector of the above. In the above-mentioned optical disk regenerative apparatus, the above-mentioned playback means reproduces the pointer in which the field in the 2nd sector by which the above-mentioned descrambling key is reproduced is shown from the 1st sector on which the data of the contents by which encryption was carried out [above-mentioned] were recorded preferably.

[0031] The optical disk recording apparatus concerning this invention to the key management information field of the record mold optical disk which can record data An acquisition means to be the optical disk recording apparatus which assigns and records the information on a descrambling key required in order to encipher the data of contents, and to acquire the information about a descrambling key required for the data of contents which should be recorded, The information on the descrambling key by which reproduced the information on the descrambling key recorded on the above-mentioned key management information field, and playback was carried out [above-mentioned], It is characterized by having the allocation means which assigns the field which records the descrambling key which should be recorded in the above-mentioned key management information field based on the information about the descrambling key by which acquisition was carried out [above-mentioned].

[0032] The optical disk recording apparatus concerning this invention to the key management information field of the record mold optical disk which can record data An acquisition means to be the optical disk recording apparatus which records the information on a descrambling key required in order to encipher the data of contents, and to acquire a descrambling key required in order to reproduce the data of contents, It is characterized by having a record means to record arranging the descrambling key by which reproduced the information on the descrambling key recorded on the above-mentioned key management information field, and acquisition was carried out [above-mentioned] based on the information on the descrambling key by which

playback was carried out [above-mentioned] in the above-mentioned key management information field.

[0033] In the optical disk recording apparatus which records the data of contents to the record mold optical disk with which the optical disk recording apparatus concerning this invention can record data the above-mentioned optical disk A playback means to reproduce disk identification information from the above-mentioned disk identification information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, A decision means to judge whether the data of contents are recordable on the above-mentioned optical disk based on the disk identification information by which playback was carried out [above-mentioned], When it is judged that the data of the above-mentioned contents are recordable on the above-mentioned optical disk The allocation means which assigns the field for recording a descrambling key required in order to encipher the data of the above-mentioned contents in the key management information field in the above-mentioned optical disk, It is characterized by having a record means to record the key index which shows the field which records the descrambling key of the data of contents which should be recorded on the same sector as the sector on which the data of the above-mentioned contents which should carry out record were recorded.

[0034] The optical disk regenerative apparatus concerning this invention from the key management information field of the record mold optical disk which can record data It is the optical disk regenerative apparatus which reproduces a descrambling key. The above-mentioned optical disk The 1st playback means which reproduces the data of the above-mentioned key management information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, A decision means to judge whether the data of the above-mentioned sector field are scrambled based on the data of the sector field in the key management information field by which playback was carried out [above-mentioned], When it is judged that the data of the above-mentioned sector field are scrambled The key index currently recorded in the same sector field as the sector field where the data of the above-mentioned sector field were recorded is reproduced. The 2nd playback means which reproduces a descrambling key from the descrambling key area shown with the key index by which playback was carried out [above-mentioned], It is characterized by having the 3rd playback means which reproduces disk identification information from the above-mentioned disk identification information field, and a decryption means to reproduce by decrypting the enciphered

descrambling key by which playback was carried out [above-mentioned], using as a key the disk identification information by which playback was carried out [above-mentioned].

[0035] In the above-mentioned optical disk regenerative apparatus, error detecting code is preferably given to the descrambling key by which the decryption was carried out [above-mentioned], the above-mentioned decryption means judges the existence of the error in the descrambling key by which the decryption was carried out [above-mentioned] based on the error detecting code given to the descrambling key by which the decryption was carried out [above-mentioned], and it judges [whether based on the above-mentioned decision result the descrambling key by which the decryption was carried out / above-mentioned / is reproduced, and].

[0036] The record actuation which records data to the data-logging playback field of the record mold optical disk with which the optical disk record playback approach concerning this invention can record data, It is the optical disk record playback approach which controls at least one side of the playback actuation which reproduces data from the above-mentioned data-logging playback field. The above-mentioned optical disk The step which reproduces the above-mentioned disk identification information from the above-mentioned disk identification information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, Based on the disk identification information by which playback was carried out [above-mentioned], it judges whether at least one of the above-mentioned record actuation and the above-mentioned playback actuation is performed, and is based on the decision result concerned. The above-mentioned record actuation, It is characterized by including the step controlled to perform at least one side of the above-mentioned playback actuation.

[0037] In the optical disk record approach which records the data of contents to the record mold optical disk with which the optical disk record approach concerning this invention can record data the above-mentioned optical disk The step which reproduces disk identification information from the above-mentioned disk identification information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, It is characterized by including the step which records the data with which at least the part was enciphered to the above-mentioned optical disk, using as a key the disk identification information by which playback was carried out [above-mentioned].

[0038] In the optical disk playback approach which reproduces the data of contents from the record mold optical disk with which the optical disk playback approach concerning

this invention can record data the above-mentioned optical disk The step which reproduces disk identification information from the above-mentioned disk identification information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, After reproducing the data with which at least the part was enciphered from the above-mentioned optical disk, it is characterized by including the step decrypted using as a key the disk identification information by which playback was carried out [above-mentioned].

[0039] The optical disk record approach concerning this invention is characterized by including the step which records the descrambling key for solving the code given to the data of the enciphered contents, and the data of the above-mentioned contents on the above-mentioned optical disk in the optical disk record approach which records the data of contents to the record mold optical disk which can record data.

[0040] The optical disk playback approach concerning this invention is characterized by including the step which reproduces the descrambling key for solving the code given to the data of the contents enciphered in the optical disk playback approach which reproduces the data of contents from the record mold optical disk which can record data, and the data of the above-mentioned contents from the above-mentioned optical disk.

[0041] The optical disk record approach concerning this invention to the key management information field of the record mold optical disk which can record data The step which acquires the information about a descrambling key required for the data of contents which are the optical disk record approach which assigns and records the information on a descrambling key required in order to encipher the data of contents, and should be recorded, The information on the descrambling key by which reproduced the information on the descrambling key recorded on the above-mentioned key management information field, and playback was carried out [above-mentioned], It is characterized by including the step which assigns the field which records the descrambling key which should be recorded in the above-mentioned key management information field based on the information about the descrambling key by which acquisition was carried out [above-mentioned].

[0042] The optical disk record approach concerning this invention to the key management information field of the record mold optical disk which can record data The step which is the optical disk record approach which records the information on a descrambling key required in order to encipher the data of contents, and acquires a descrambling key required in order to reproduce the data of contents, It is characterized by including the step recorded as arranging the descrambling key by which reproduced

the information on the descrambling key recorded on the above-mentioned key management information field, and acquisition was carried out [above-mentioned] based on the information on the descrambling key by which playback was carried out [above-mentioned] in the above-mentioned key management information field.

[0043] In the optical disk record approach which records the data of contents to the record mold optical disk with which the optical disk record approach concerning this invention can record data the above-mentioned optical disk The step which reproduces disk identification information from the above-mentioned disk identification information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, The step which judges whether the data of contents are recordable on the above-mentioned optical disk based on the disk identification information by which playback was carried out [above-mentioned], When it is judged that the data of the above-mentioned contents are recordable on the above-mentioned optical disk The step which assigns the field for recording a descrambling key required in order to encipher the data of the above-mentioned contents in the key management information field in the above-mentioned optical disk, It is characterized by including the step which records the key index which shows the field which records the descrambling key of the data of contents which should be recorded on the same sector as the sector on which the data of the above-mentioned contents which should carry out record were recorded.

[0044] The optical disk playback approach concerning this invention from the key management information field of the record mold optical disk which can record data It is the optical disk playback approach which reproduces a descrambling key. The above-mentioned optical disk The step which reproduces the data of the above-mentioned key management information field including the disk identification information field which records the disk identification information for identifying the above-mentioned optical disk, The step which judges whether the data of the above-mentioned sector field are scrambled based on the data of the sector field in the key management information field by which playback was carried out [above-mentioned], When it is judged that the data of the above-mentioned sector field are scrambled The key index currently recorded in the same sector field as the sector field where the data of the above-mentioned sector field were recorded is reproduced. The step which reproduces a descrambling key from the descrambling key area shown with the key index by which playback was carried out [above-mentioned], It is characterized by including the step which reproduces disk identification information from the above-mentioned disk identification information field, and the step reproduced

by decrypting the enciphered descrambling key by which playback was carried out [above-mentioned], using as a key the disk identification information by which playback was carried out [above-mentioned].

[0045] The optical disk concerning this invention is characterized by including the 1st information field which records the 1st disk information, the 2nd information field which records the 2nd disk information for identifying each optical disk, and the user data area which records information data by irradiating a light beam to the field concerned in the record mold optical disk which can record data.

[0046] In the above-mentioned optical disk, the 2nd disk information of the above is recorded by being a long configuration and removing radially, the record film in the information field of the above 2nd selectively in two or more fields preferably. Moreover, in the above-mentioned optical disk, preferably, the information field of the above 2nd is arranged in the information field of the above 1st, it is arranged at the inner circumference side of the information field of the above 1st, or the information field of the above 2nd is arranged over another field located in an inner circumference side rather than some fields in the information field of the above 1st, and the information field of the above 1st. Furthermore, the 1st disk information of the above is preferably recorded in the form of a very small concavo-convex pit.

[0047] In the record mold optical disk with which the optical disk concerning this invention can record data the above-mentioned optical disk It has the sector structure equipped with two or more sectors. Each above-mentioned sector A sector header field and the Maine data area which records the enciphered data are included. The above-mentioned sector header field In order to decrypt the data by which encryption was carried out [above-mentioned], size of the above-mentioned decode key information field is characterized by being smaller than the size of each above-mentioned decode key including the decode key information field which records at least one decode key which is the need.

[0048] In the above-mentioned optical disk, each above-mentioned decode key is preferably divided into two or more division decode keys which have predetermined size, and two or more above-mentioned division decode keys are recorded on each decode key information field of two or more continuous sectors. Here, the number of partitions of the above-mentioned decode key is a divisor of the number of sectors preferably contained in the error correcting code (ECC) block which are two or more sectors required for an error correction. Moreover, in the above-mentioned optical disk, the index which shows the record location in the above-mentioned decode key table of a decode key required in order to record each above-mentioned decode key on the decode

key table which has two or more decode keys preferably and to decrypt the data by which encryption was carried out [above-mentioned] is recorded on the decode key information field of the above-mentioned sector. Furthermore, in the above-mentioned optical disk, the decode key condition field which recorded the decode key condition of expressing the record condition of the above-mentioned decode key table and of preferably as information as opposed to each decode key field of the above-mentioned decode key table is recorded. Furthermore, in the above-mentioned optical disk, the above-mentioned decode key table is preferably recorded over two or more different error correcting code (ECC) blocks. Moreover, in the above-mentioned optical disk, each above-mentioned decode key is preferably managed and recorded in one [at least] unit of the file unit managed in a file management field, and the extent units which consist of two or more sectors which continue on an optical disk.

[0049] In the record mold optical disk with which the optical disk concerning this invention can record data the above-mentioned optical disk The Maine data area which records data is included. The above-mentioned Maine data area The non-enciphering field which records data in the state of un-enciphering, and the encryption field which records data in the state of encryption are included. The above-mentioned non-enciphering field The data of the above-mentioned encryption field are characterized by being enciphered using the decode key changed using the above-mentioned decode key translation data including the decode key translation data used for conversion of the decode key for decrypting data.

[0050] In the above-mentioned optical disk preferably the above-mentioned Maine data area The control information record sector which records the control information used for playback control of data in the state of un-enciphering, The data of the above-mentioned data-logging sector are enciphered using the decode key changed using the above-mentioned decode key translation data including the decode key translation data with which the above-mentioned control information record sector is used for conversion of the above-mentioned decode key including the data-logging sector which records data in the state of encryption. In the above-mentioned optical disk moreover, preferably The non-enciphering field where the above-mentioned data-logging sector records data in the state of un-enciphering, The above-mentioned non-enciphering field contains another decode key translation data including the encryption field which records data in the state of encryption. AV data of the above-mentioned encryption field are enciphered using the decode key into which the decode key changed using the above-mentioned decode key translation data was changed using 2nd still more nearly another decode key translation data. Furthermore,

in the above-mentioned optical disk, the above-mentioned decode key translation data includes copy-of-data control information at least preferably.

[0051] In the optical disk record approach for the optical disk record approach concerning this invention to record data on the record mold optical disk which can record data When it is judged that there are a step which judges whether the decode key status recorded on the above-mentioned optical disk is read, and there is any free area of a decode key based on the decode key status by which reading appearance was carried out [above-mentioned], and a free area of the above-mentioned decode key The step which reserves a decode key field and records a decode key, and the step which sets up copyright control information and a decode key index in one [at least] unit of a file unit and the extent units, The step which enciphers data using the above-mentioned decode key, and records the enciphered data on the above-mentioned optical disk in one [at least] unit of a file unit and the extent units, It is characterized by including the step which records the file management information for managing the data recorded on the above-mentioned optical disk on the above-mentioned optical disk.

[0052] In the optical disk playback approach for the optical disk playback approach concerning this invention to reproduce data from the record mold optical disk which can record data The step which reproduces and acquires a decode key index from the record section of the data which were recorded per the file unit or extent, and which should be reproduced, It is characterized by including the step which reproduces and acquires the decode key corresponding to the decode key index by which acquisition was carried out [above-mentioned], and the step which reproduces the data of the file unit enciphered using the above-mentioned decode key, or an extent unit.

[0053] In the optical disk deletion approach for the optical disk deletion approach concerning this invention to delete data from the record mold optical disk which can record data The step which reproduces and acquires a decode key index from the record section of the data which were recorded per the file unit or extent, and which should be deleted, The step which corresponds to the decode key index by which acquisition was carried out [above-mentioned], updates the decode key status which shows the record condition of a decode key, and opens a decode key, It is characterized by including the step which updates the above-mentioned file management information by deleting the file entry corresponding to the above-mentioned data which should carry out deletion from the file management information for managing the data recorded on the above-mentioned optical disk.

[0054] The data encryption equipment with which the information processing system concerning this invention enciphers data using a cryptographic key, The optical disk

record regenerative apparatus which records a decode key required in order to decrypt the above-mentioned data on a record mold optical disk, and is reproduced, It is the information processing system equipped with the control device connected to the above-mentioned optical disk record regenerative apparatus and the above-mentioned data encryption equipment. The above-mentioned optical disk record regenerative apparatus The 1st record playback means which records a decode key table on the above-mentioned optical disk, and reproduces a decode key table from the above-mentioned optical disk, Encryption and the decryption means of receiving and decrypting the decode key which enciphered the above-mentioned decode key, transmitted to the above-mentioned control unit and was enciphered from the above-mentioned control unit, The decode key condition table showing the record condition of a decode key in the above-mentioned optical disk is recorded. It has the 2nd record playback means which reproduces a decode key condition table from the above-mentioned optical disk. The above-mentioned data encryption equipment It has an encryption means to encipher the above-mentioned decode key and to transmit to the above-mentioned control unit. The above-mentioned control unit A receiving means to receive the decode key enciphered from the encryption means of the above-mentioned data encryption equipment, The free area of a decode key is searched based on the decode key condition table by which playback was carried out [above-mentioned]. The enciphered decode key by which reception was carried out [above-mentioned] is assigned to the free area by which retrieval was carried out [above-mentioned]. It has an allocation means to transmit the enciphered decode key which was assigned the account of a top to the above-mentioned optical disk record regenerative apparatus. Encryption and the decryption means of the above-mentioned optical disk record regenerative apparatus It is characterized by receiving and decrypting the enciphered decode key which was assigned the account of a top from the allocation means of the above-mentioned control unit.

[0055] The optical disk regenerative apparatus which reproduces the decode key table equipped with two or more decode keys required in order that the information processing system concerning this invention may decrypt data and the above-mentioned data from a record mold optical disk, It is the information processing system equipped with the control device connected to the above-mentioned optical disk regenerative apparatus, and the data decryption equipment which decrypts data using a decode key. The above-mentioned optical disk regenerative apparatus The decode key table by which playback was carried out [above-mentioned] is enciphered as the 1st playback means which reproduces a decode key table from the above-mentioned optical disk. An

encryption means to transmit the enciphered decode key table to the above-mentioned control unit, It has the 2nd playback means which reproduces the decode key condition table showing the record condition of two or more decode keys from the above-mentioned optical disk. The above-mentioned control unit A receiving means to receive the decode key table by which encryption was carried out [above-mentioned] from the above-mentioned optical disk regenerative apparatus, It has a retrieval means to search the enciphered decode key required in order to decrypt the data recorded on the above-mentioned optical disk from the decode key table by which reception was carried out [above-mentioned] based on the decode key condition table by which playback was carried out [above-mentioned], and to transmit to the above-mentioned data decryption means. The above-mentioned data decryption equipment It is characterized by having the 1st decryption means which decrypts the decode key by which encryption was carried out [above-mentioned], and generates a decode key, and the 2nd decryption means which decrypts the enciphered data which were reproduced with the optical disk regenerative apparatus using the decode key by which the decryption was carried out [above-mentioned].

[0056] In the optical disk recording apparatus which records data on the record mold optical disk with which the optical disk recording apparatus concerning this invention can record data the above-mentioned optical disk The data containing the decode key translation data used for conversion of the decode key for decrypting data are recorded on the above-mentioned non-enciphering field in the state of un-enciphering including a non-enciphering field and an encryption field. It is characterized by having a record means to record the data enciphered using the decode key changed using the above-mentioned decode key translation data on the above-mentioned encryption field.

[0057] In the above-mentioned optical disk recording device preferably The above-mentioned optical disk contains a control information record sector and a data-logging sector. The above-mentioned record means The control information used for playback control of the above-mentioned data is recorded on the above-mentioned control information record sector in the state of un-enciphering. It changes into the decode key into which the cryptographic key was changed using the decode key translation data contained in the above-mentioned control information, data are enciphered using the decode key by which conversion was carried out [above-mentioned], and it records on the above-mentioned data-logging sector. Moreover, the above-mentioned record means records the data which contain another decode key translation data preferably on the non-enciphering field of the above-mentioned data-logging sector in the state of un-enciphering, and it changes to

the decode key into which a cryptographic key was changed using the decode key translation data contained in the above-mentioned control information, and the decode key translation data according to above, data encipher using the decode key by which conversion was carried out [above-mentioned], and it records to the above-mentioned data-logging sector in the above-mentioned optical disk recording apparatus.

[0058] In the optical disk regenerative apparatus which reproduces data from the record mold optical disk with which the optical disk regenerative apparatus concerning this invention can record data the above-mentioned optical disk It carries out having had a playback means decrypts the data which changed into the decode key into which the decode key was changed using the decode key translation data recorded on the above-mentioned non-enciphering field, and were recorded on the above-mentioned encryption field using the decode key by which conversion was carried out [above-mentioned], and reproduce, including the non-enciphering field and the encryption field as the description.

[0059] In the above-mentioned optical disk regenerative apparatus preferably The above-mentioned optical disk contains a control information record sector and a data-logging sector. The above-mentioned playback means The control information used for playback control of the above-mentioned data is reproduced from a control information record sector. The data which changed into the decode key into which the decode key was changed using the decode key translation data contained in the above-mentioned control information, and were recorded on the above-mentioned data-logging sector using the decode key by which conversion was carried out [above-mentioned] are decrypted, and it reproduces. In the above-mentioned optical disk regenerative apparatus moreover, the above-mentioned playback means The decode key translation data which reproduces preferably another decode key translation data recorded on the non-enciphering field of the above-mentioned data-logging sector, and is contained in the above-mentioned control information, The data which changed into the decode key into which the decode key was changed using another decode key translation data by which playback was carried out [above-mentioned], and were recorded on the above-mentioned data-logging sector using the decode key by which conversion was carried out [above-mentioned] are decrypted, and it reproduces.

[0060] In the optical disk record approach which records data on the record mold optical disk with which the optical disk record approach concerning this invention can record data the above-mentioned optical disk The data containing the decode key translation data used for conversion of the decode key for decrypting data are recorded on the

above-mentioned non-enciphering field in the state of un-enciphering including a non-enciphering field and an encryption field. It is characterized by including the step which records the data enciphered using the decode key changed using the above-mentioned decode key translation data on the above-mentioned encryption field.

[0061] In the optical disk playback approach which reproduces data from the record mold optical disk with which the optical disk playback approach concerning this invention can record data the above-mentioned optical disk It carries out containing the step which decrypts the data which changed into the decode key into which the decode key was changed using the decode key translation data recorded on the above-mentioned non-enciphering field, and were recorded on the above-mentioned encryption field using the decode key by which conversion was carried out [above-mentioned], and is reproduced including a non-enciphering field and an encryption field as the description.

[0062] In the mold optical disk only for playbacks for the optical disk concerning this invention to reproduce the recorded data The data playback field where data were recorded, and the disk identification information field only for playbacks where the disk identification information for identifying the above-mentioned optical disk was recorded are included. The above-mentioned data playback field It is characterized by including the field where the data enciphered using the information containing the disk identification information for identifying the above-mentioned optical disk as a key were recorded.

[0063] In the mold optical disk only for playbacks for the optical disk concerning this invention to reproduce the recorded data the above-mentioned optical disk The data playback field where data were recorded is included. The above-mentioned data playback field It is characterized by including the field where the descrambling key for solving the code given to the data of the contents which are at least one side of the music data enciphered as the enciphered image data, and the data of the above-mentioned contents was recorded.

[0064] In the mold optical disk only for playbacks for the optical disk concerning this invention to reproduce the recorded data The disk identification information field only for playbacks where the disk identification information for identifying the above-mentioned optical disk was recorded, The data playback field where the data of the contents containing at least one of the enciphered image data and the enciphered music data were recorded, It is characterized by including the key management information field where the key information used when reproducing the data of the above-mentioned contents, and the descrambling key enciphered using the

above-mentioned disk identification information as a key were recorded.

[0065] In the mold optical disk only for playbacks for the optical disk concerning this invention to reproduce the recorded data the above-mentioned optical disk It has the sector structure equipped with two or more sectors. Each above-mentioned sector A sector header field and the Maine data area where the enciphered data were recorded are included. The above-mentioned sector header field In order to decrypt the data by which encryption was carried out [above-mentioned], size of the above-mentioned decode key information field is characterized by being smaller than the size of each above-mentioned decode key including the decode key information field where at least one decode key which is the need was recorded.

[0066]

[Embodiment of the Invention] Hereafter, the operation gestalt which starts this invention with reference to a drawing is explained.

[0067] <Operation gestalt of ** 1st> drawing 1 is the top view showing the data storage area of the record mold optical disk 100 which is the 1st operation gestalt concerning this invention. This record mold optical disk 100 is the record medium which can record digital data, and contains a write once optical disk and an erasable optical disk.

[0068] the lead-in groove field where, as for 101, the management information of an optical disk 100 was recorded in drawing 1 , and 102 -- image data (a still picture and an animation are included.), such as a film, and a sound -- the user data area where the digital data which needs protection of copyrights, such as contents of AV data containing at least one side of which easy voice data and software of a computer, is recorded, and 103 are lead-out fields where defective management information etc. is recorded. The lead-in groove field 101 is constituted by the field 104 only for playbacks recorded in the form of PURIPITTO, and the record playback field 105 which is a rewritable field which has a guide slot. Here, the control area which described the physical property of an optical disk 100 is recorded on the field 104 only for playbacks by the manufacturer in the form of PURIPITTO. The management information for managing the defect on data and the optical disk 100 for the write-in test by the optical disk recording apparatus etc. is recorded on the lead-out field 103 or the rewritable field 105 by the optical disk recording apparatus. Furthermore, as disk individual information, BCA106 is added to an optical disk 100 at the inner circumference side of the field 104 only for playbacks of the lead-in groove field 101, after the optical disk 100 with which it is a well-known approach as shown below, and contents were recorded is completed.

[0069] Drawing 2 (a) is the block diagram and drawing of longitudinal section showing the equipment configuration when forming BCA106 of the optical disk 100 of drawing 1 ,

and drawing 2 (b) is a graph which shows drawing of longitudinal section of the optical disk 100 after forming BCA106 of the optical disk 100 of drawing 1 , and the reinforcement of the reflected light which receives horizontally. The example of the optical disk 100 of a double-sided record mold is shown, between two substrates 201,207, a recording layer 202, a reflecting layer 203, a glue line 204, a reflecting layer 205, and a recording layer 206 are inserted, and an optical disk 100 consists of drawing 2 (a) and drawing 2 (b).

[0070] When recording BCA on an optical disk 100, as shown in drawing 2 (a), the data of the shape of a stripe which carried out the phase-encoding modulation (phase encoding modulation) are recorded on a pit in piles by irradiating the laser beam from the high-power laser light source 211 in the shape of a pulse through the focal lens 212 at the reflecting layer 205 of an optical disk 100, and removing some reflecting layers 205. At the time of playback, as shown in drawing 2 (b), after it is reproduced intermittently and the signal with which the amount of reflected lights fell in the part from which the reflecting layer 205 is removed makes binary the reproduced signal, the data of BCA are reproduced by carrying out a phase-encoding recovery (phase encoding demodulation). the disk identifier which is peculiar information can be recorded every optical disk 100, and BCA created by such recording method cannot be altered further -- etc. -- it has the description.

[0071] Drawing 3 is drawing showing a record format of drawing 1 of BCA106. As shown in drawing 3 , in order that the synchronous code 301, an error detection code 302, an error correction code 303, etc. may improve the rate of reading of the BCA data 304, it is recorded on BCA106. The disk identification information 305 is constituted by connecting two or more of these BCA data 304. The classification of the classification of data recordable on a user data area and the classification of data refreshable from a user data area are recorded on the disk identification information 305. Since the data of BCA106 cannot be altered, they can give a fixed limit to a user's disk activity by the disk identification information recorded at the time of manufacture of an optical disk 100.

[0072] Drawing 4 is drawing showing the sector structure of the sector data 401 in the user data area 102 of drawing 1 . In drawing 4 , the user data area 102 of drawing 1 has the accessible sector structure in the unit of a constant rate, and the sector data 401 is constituted by a header 402, the Maine data 403, and the error detection code 404.

[0073] Here, the Maine data 403 are a field where AV data, the data of a computer, etc. are recorded. Moreover, data (Data Identifier) ID 405, the ID error detection code 406, the scramble control information 407, the key information 408, etc. are recorded on a header 402. The logical address for identifying a sector etc. is recorded on data ID 405,

and the ID error detection code 406 is a code for [of Data ID] carrying out error detection. Moreover, the scramble control information 407 is a flag which shows the Maine data whether the scramble is given or not, and the information about the key for the key information 408 descrambling the Maine data is recorded. The key index (1st operation gestalt) which is a pointer to the descrambling key recorded on the descrambling key (modification of the 1st operation gestalt) itself and another field on an optical disk 100 as information about a key is recorded. The example of drawing 4 shows the case where the key index for referring to the descrambling key recorded on the key management information field 107 of drawing 1 which is another field on an optical disk 100 is recorded.

[0074] Drawing 5 is drawing showing the configuration of the key management information field 107 of drawing 1 . In drawing 5 , the key management information field 107 consists of a key information field 501, a contents information field 502, and a key-index list field 503.

[0075] In the key information field 501, while several 504 of a used descrambling key area is recorded, the key information field 501 includes the descrambling key area 505 which is a field which records the descrambling key for solving the scramble given to AV data etc., and the key status field 506 which records the record condition (finishing [intactness, field reserved, and record] etc. is shown.) of the descrambling key recorded on the descrambling key area 505. Two or more descrambling keys are recorded on the descrambling key area 505, the key index showing the storing location in the inside of the descrambling key area 505 is recorded on the key-index list field 503, and the key index concerned can refer two or more above-mentioned descrambling keys. The status information which expresses the record condition of a previous descrambling key to the key status field 506 is stored in the location which can be referred to with a key index.

[0076] What has required protection of copyrights is registered into the contents information field 502 in the contents recorded on an optical disk 100, and the information about the key used from contents with it is registered into it. 507 contents with which the contents information field 502 is registered into the key-index list field 503, and the contents information 508 for several contents minutes are recorded. Furthermore, the content ID for identifying contents, the number of the descrambling key used from the contents, and the pointer to the key-index list 509 which recorded the key to be used are recorded on the contents information 508. The key-index list field 503 is a field which records the index for referring to the key used from contents by the list form in a contents unit. The key index which refers to the record section of all the descrambling keys currently used from contents is recorded on the key-index list field

503.

[0077] Thus, as information as which rewriting expresses the service condition of a disk to difficult disk identification information, by recording a local identifier, a data category identifier, a disk identifier, etc. at the time of manufacture, an optical disk record regenerative apparatus detects such information, and it makes it possible to control record actuation and playback actuation according to the protection level and the utilization level of copyright which contents have in the constituted record mold optical disk 100. Moreover, although a user data area can be copied even when the contents by which protection of copyrights was carried out to another optical disk are copied since rewriting is recorded by the difficult approach and modification by the side of a user cannot be performed, disk identification information cannot be copied. Therefore, by recording the data scrambled using disk identification information on an optical disk, in the optical disk which has different disk identification information, the user data area which cannot descramble exists and right playback cannot be performed.

[0078] When recording a local identifier in the 1st operation gestalt at the time of record of contents, drawing 15 (a) in the same area Are drawing showing whether the copy and playback of contents are possible in an area which is different in a list, and when the local identifier is beforehand recorded in the 1st operation gestalt at the time of shipment of an optical disk, drawing 15 (b) in the same area It is an area which is different in a list, and is drawing showing whether the copy and playback of contents are possible.

[0079] For example, as shown in drawing 15 (a), when local identification code is not recorded at the time of shipment of an optical disk but the local identifier to which contents express an available area at the time of record of contents is recorded on record and a playback field, utilization in other areas can be prevented. However, record of contents is possible also on the disk (for the areas RC 2 in drawing 15 (a)) which should be used in other areas, and playback of contents is surely possible. In the record medium in which the digital copy of contents is possible, in order to protect a copyright person's profit, a pricing system etc. is provided, and at the time of a sale of an optical disk, it is added to a tariff and collected. However, the pricing added has possibility of not being correctly distributed to the copyright person who should get a profit essentially, when the record medium which should be used in other countries is used unjustly, since it differs for every country.

[0080] Moreover, as shown in drawing 15 (b), the copy and playback of the contents to an optical disk which should be used in other areas can be prevented by recording by the approach which a local identifier cannot alter beforehand at the time of shipment of an

optical disk. Similarly, when a data category identifier is recorded as disk identification information, record, and the copy and playback of the contents to a refreshable disk can be restricted for data by comparing with the category identifier which the data to record have. When a peculiar disk identifier is recorded as disk identification information the whole optical disk, the data to record can be enciphered by the disk identifier and suppose that it is available only with the optical disk.

[0081] In this operation gestalt, AV data which need protection of copyrights, and computer data are sufficient as the data scrambled by disk identification information, and the descrambling key for solving the scramble given to AV data and computer data is sufficient as them.

[0082] Drawing 13 is the block diagram showing the approach for judging whether it is the descrambling key of normal from the encryption descrambling key concerning the modification of the 1st operation gestalt. As shown in drawing 13 , the encryption descrambling key calculated by scrambling the data which added the error detecting code for detecting the error of a descrambling key to the descrambling key using disk identification information may be recorded on an optical disk. In an optical disk regenerative apparatus, it judges whether the descrambling key decoded by decoding an encryption descrambling key to a descrambling key and error detecting code, and carrying out error detection based on the parity check in the decoded error detecting code etc. is the thing of normal. For example, since it can judge that it is not the descrambling key of normal by generating the mistaken descrambling key and checking error detecting code when it descrambles by different disk identification information, an unjust copy is detectable.

[0083] In addition, you may make it give a utilization limit different the whole optical disk created from different La Stampa by preparing La Stampa which created two or more kinds of disk identification information by PURIPITTO as an option which records disk identification information, and creating an optical disk from each. Furthermore, by recording the disk identification information scrambled by scrambling disk identification information using a private key on the optical disk, a user does not understand the protection level of the copyright described by disk identification information, and it is made into him, consequently protection of copyrights is strengthened more.

[0084] The case (1st operation gestalt) where the key index which is a pointer to the descrambling key recorded on another field the case (modification of the 1st operation gestalt) where the descrambling key itself is recorded as information about the key explained in drawing 4 , and on a disk is recorded is explained with reference to

drawing 6 (a) and drawing 6 (b). Here, drawing 6 (a) is the block diagram concerning the modification of the 1st operation gestalt showing the record approach which records a descrambling key and AV data to the sector data 401 of drawing 1 , and drawing 6 (b) is the block diagram concerning the 1st operation gestalt showing the record approach which records the key index and AV data to a descrambling key to the sector data 401 of drawing 1 .

[0085] The descrambling key which is key information 408a required in order to descramble the Maine data 403 and the Maine data 403 at the same sector data 401 in the case of drawing 6 (a) is recorded. For this reason, it is necessary to acquire a descrambling key required for descrambling at the time of record of AV data. That is, acquisition and purchase of the key itself are indispensable at the time of record of AV data.

[0086] The key index which is the key information 408 which refers to the descrambling key area which records information required for the same sector data 401 in order to descramble the Maine data 403 and the Maine data 403 on the other hand in the case of drawing 6 (b) is recorded, and a descrambling key is recorded on the field specified with a key index. At the time of record of AV data, the key ID which shows by which key in the key used from the contents to record data can be descrambled is acquired, the key information 408 which is a key index corresponding to Key ID is acquired from the key-index list included in contents information, and it records with the Maine data 403. When record of a descrambling key receives a descrambling key, it is performed, and it is recorded on the descrambling key area shown by the key index corresponding to Key ID. Consequently, record of the descrambling key corresponding to AV data and it can be performed independently. That is, record of AV data, acquisition of a key, or purchase can be performed independently, and acquisition or purchase of a key is necessarily less necessary at the time of record of AV data. The user records contents, and in case it reproduces actually, the directions of him that a key comes to hand become possible.

[0087] Drawing 14 is drawing concerning the modification of the 1st operation gestalt showing the configuration of a descrambling field managed table. Although the case where the key index for referring to a descrambling key was recorded on the same sector data 401 was explained since the descrambling key for solving the enciphered contents and its code in the above operation gestalt was associated, the descrambling field managed table of drawing 14 which manages the response relation of the address range and descrambling key which are the sector on which the enciphered contents are recorded may be used. On this descrambling field managed table, when the address range which is the sector on which the enciphered contents are recorded is expressed

with a starting address and an ending address and reproduces the data of those sectors, the enciphered contents are descrambled with reference to a descrambling key.

[0088] In order to acquire the contents to record and the descrambling key used there, the content ID which makes contents identifiable is used. It is recorded as a list of descrambling keys used from content ID and its contents into the contents information recorded on the contents management list of [in the contents information field 502 recorded on the optical disk as shown in drawing 5]. By taking the list configuration which can use two or more descrambling keys to one contents, service which some contents and software sell by the piece is attained.

[0089] Moreover, in the modification mentioned above with reference to drawing 13 , when the data which scrambled the descrambling key to which error detection codes, such as a checksum and a Cyclic Redundancy Check sign, were added by disk identification information are unjustly copied to other disks, it is detected as an error by descrambling by different disk identification information. In such a case, the descrambling key scrambled by the disk identification information currently recorded on the optical disk in this descrambling key can come to hand, and the disk which can be played correctly can also be created by transposing to it.

[0090] The key management information field 107 of drawing 1 is recorded on the rewritable lead-in groove field 101. Usually, the user data area 102 consists of a user area accessible from the drive equipment of a personal computer, and a spare field to the defective sector on an optical disk, and only its user area is accessible as a logical continuation field in a usual read-out command and a usual write command. By arranging key management information to the lead-in groove field 101, it can prevent that direct access is carried out from the drive equipment of a personal computer etc., and acquisition of the key for solving the scramble given to AV data etc. from the personal computer can be made impossible.

[0091] <Operation gestalt of ** 2nd> drawing 7 is the block diagram showing the configuration of the optical disk record regenerative apparatus which is the 2nd operation gestalt concerning this invention. This optical disk record regenerative apparatus is equipment which records the contents of AV data, such as image data, music data, etc. which need protection of copyrights for the optical disk 100 concerning the 1st operation gestalt.

[0092] The optical head which is the optical pickup by which the optical disk of the 1st operation gestalt and 702 are constituted for 701 from semiconductor laser and an optical element in drawing 7 , The record playback control circuit where 703 performs motion control of semiconductor laser, and binary-ization of a regenerative signal, Error

detection of an error and correction processing in which the strange demodulator circuit which carries out the digital recovery of the regenerative signal made binary while 704 carried out digital modulation of the digital data which should be recorded, and 705 occurred with a blemish, dust, etc. on an optical disk 701, The error detection and the correction circuit which perform generation processing of an error correcting code required for error detection and correction processing, The buffer memory which is RAM which uses 706 as the operating memory and data buffer memory of error detection and the correction circuit 705, The descrambling circuit which descrambles AV data which 707 is scrambled and are recorded, The MPEG decoder circuit which elongates the video data which 708 was compressed and was recorded, The output circuit which 709 carries out D/A conversion of the elongated image data, and generates and outputs a video signal and an audio signal, The control CPU whose 710 controls actuation of the whole optical disk record regenerative apparatus The communication circuit which acquires the descrambling key which solves the code in which 711 was given to contents, and 712 are data receiving circuits which receive digital data of the enciphered contents, such as image data and music data, from communication terminals, such as a set top box.

[0093] The data-logging actuation in the optical disk record regenerative apparatus of drawing 7 constituted as mentioned above is explained. Digital data of the enciphered contents, such as image data transmitted from communication terminals, such as a set top box and an MPEG encoder, and music data, are temporarily saved at buffer memory 706, after being received by the data receiving circuit 712. Error detection and the correction circuit 705 generate detection, the error detection required for correction processing, and the correction code of the error resulting from a blemish, dust, etc. of an optical disk 701 to the saved digital data of contents, and reconfigurate record data to it. Signs, such as a well-known Reed Solomon code, are used for error detection and a correction code, for example. Here, the reconfigurated record data contain digital data, and the error detection and the correction code of contents. Modulation techniques, such as 8/16 modulation technique, are used for the strange demodulator circuit 704 in the case of record, and it carries out digital modulation of the record data. And the record playback control circuit 703 records record data on an optical disk 701 by carrying out intensity modulation of the power of the laser beam outputted from the optical head 702 according to the record data by which digital modulation was carried out, and irradiating the laser concerned at an optical disk 701.

[0094] Drawing 8 is a flow chart which shows record processing of AV data performed by the control CPU 710 of the optical disk record regenerative apparatus of drawing 7 .

[0095] In drawing 8 , it judges whether the digital data of contents which it is going to

record now is recordable from the classification of data recordable on the user data area 102 which reproduces the disk identification information of the lead-in groove field 101, and is subsequently first recorded on disk identification information in step S802 in advance of record of AV data from an optical disk 701 in step S801. While progressing to step S803 at step S802 at the time of YES, when it is NO, record actuation is stopped by step S810, and record processing of the AV data concerned is ended.

[0096] At step S803, the data which are the sector on which key management information was recorded in the lead-in groove field 101 are reproduced, the field to key information required for record of contents assigns the reproduced key management information at step S804, and it judges whether it is ending. It progresses to step S806, after assigning the field for recording key information on the key management information field 107, when it is NO at step S804. On the other hand, it progresses to step S806 as it is at step S804 at the time of YES.

[0097] In recording contents, the control CPU 710 of an optical disk record regenerative apparatus receives the information about the data of the enciphered contents to record, and the descrambling key for solving a code through the data receiving circuit 712 from a communication terminal. Here, the information about a key is the key ID which shows to the key of what position it corresponds among the key itself used from contents, or the key used from the whole contents. It changes into the key index which is the pointer in which the field where the descrambling key corresponding to Key ID is recorded in the received key ID at step S806 when Key ID is received is shown, and the changed descrambling key is arranged to the header field of a sector to which the data of the contents decoded by the descrambling key are recorded. And at step S807, control CPU 710 performs processing of the following record data by controlling the record playback control circuit 703, the strange demodulator circuit 704, and error detection and the correction circuit 705. While carrying out digital modulation of the sector data with which error detection and the code for correction were added to sector data to record, and these codes were added using modulation techniques, such as 8/16 well-known modulation technique, and controlling the optical head 702 by this processing in a predetermined record location, intensity modulation of the laser beam is carried out according to the record data by which digital modulation was carried out. By this, record data are recorded on an optical disk 701. Furthermore, at step S808, it judges whether it is termination of record of contents, and when it is NO, return and the above-mentioned processing are repeated to step S806. If it is YES at step S808, at step S809, the updated key management information will be recorded on the key management information field 107 on an optical disk 701, and record processing of the

AV data concerned will be ended.

[0098] Drawing 9 is a flow chart which shows quota processing of the key management information field performed by the control CPU 710 of the optical disk record regenerative apparatus of drawing 7 . This processing is processing which assigns the field for recording a descrambling key in advance of record of the data of contents.

[0099] In drawing 9 , the information (the number of the descrambling key to be used etc. is included.) about the key of contents recorded from an electronic program guide etc. is first acquired in step S901. Subsequently At step S902, reproduce the key management information in the key management information field 107 currently recorded on the optical disk 701, and it sets to step S903. It judges whether the descrambling key which investigates the free area of the descrambling key area 505 from the key status field 506, and uses it from the contents which it is going to record is recordable. When it is NO at step S903, record actuation is stopped by step S907, and the quota processing concerned is ended. On the other hand, when it is YES at step S903, in order to register into the contents list of [in the contents information field 502] the contents which are step S904 and are recorded and to reserve a field required for record of a descrambling key to the descrambling key area 505 in step S905, the field for record is assigned by setting a field reserved flag as a key status field. Furthermore, after creating the key index which shows the field assigned in order to record a descrambling key as a key list and assigning the pointer as contents information at step S906, the quota processing concerned is ended.

[0100] Drawing 10 is a flow chart which shows record processing of the descrambling key performed by the control CPU 710 of the optical disk record regenerative apparatus of drawing 7 . This record processing is processing for acquiring a descrambling key from a key management pin center,large, and recording on an optical disk 701.

[0101] In drawing 10 , first, after reproducing the disk identification information of the lead-in groove field 101 of an optical disk 701 in step S1001, in order to acquire a descrambling key from a key management pin center,large in step S1002, the key ID for discriminating a key required for descrambling of desired contents from disk identification information is transmitted to a key management pin center,large through a communication circuit 711. In the key management pin center,large, a descrambling key required for descrambling of contents is chosen from the given key ID, and using information, such as sent disk identification information, a descrambling key is enciphered and a letter is answered.

[0102] After acquiring the descrambling key corresponding to Key ID from a key management pin center,large through a communication circuit 711 at step S1003, at

step S1004, the data of the key management information field 107 are reproduced, and the key index which shows the field which records a descrambling key is acquired from the key-index list shown by Key ID among the data in the reproduced key management information field 107. Subsequently, in step S1005, the acquired flag which shows key acquisition ending is set as the key status field 506 which arranges the descrambling key which carried out [above-mentioned] acquisition to the descrambling key area shown by the key index, and is equivalent to it. Furthermore, it is judged at step S1006 whether acquisition of all keys was completed, and if it is NO, processing of the return above will be repeated to step S1003. On the other hand, when it is YES at step S1006, in step S1007, the updated key management information is recorded on the key management information field 107, and record processing of the descrambling key concerned is ended.

[0103] Subsequently, data playback actuation of the optical disk record regenerative apparatus of this operation gestalt is explained with reference to drawing 7 . The digital data recorded on the optical disk 701 is reproduced as follows. The laser beam from the semiconductor laser of the optical head 702 is irradiated by the optical disk 701, and the reflected light then reflected with an optical disk 701 carries out incidence to the record playback control circuit 703 through the optical head 702. After the record playback control circuit 703 carries out photo electric translation of the reflected light which carries out incidence, by performing magnification and binary-ized processing, it generates the digitized regenerative signal and outputs it to the strange demodulator circuit 704. The strange demodulator circuit 704 carries out a digital recovery, and outputs the signal by which digital modulation was carried out using modulation techniques, such as 8/16 well-known modulation technique, on the occasion of record to a digital signal in error detection and the correction circuit 705. Subsequently, error detection and the correction circuit 705 perform the detection and correction processing of an error which originate [dust / of an optical disk 701 / a blemish dust, etc.], using buffer memory 706 as operating memory. This error detection and correction processing are performed by decoding a known Reed Solomon code etc.

[0104] Error detection and the playback data by which correction processing was carried out are outputted to the descrambling circuit 707, in order to perform descrambling processing. After the descrambling circuit 707 performs descrambling processing to playback data using the descrambling key of the key management information field 107 beforehand reproduced in advance of playback of data, it is outputted to the MPEG decoder circuit 708. Subsequently, the MPEG decoder circuit 708 outputs the data after expanding to an output circuit 709, after elongating the video data and music data

which were compressed. Furthermore, an output circuit 709 carries out D/A conversion of the elongated data which are inputted to a video signal and an audio signal, and outputs them to the device of high orders, such as a TV apparatus and audio equipment.

[0105] Drawing 11 is a flow chart which shows regeneration of AV data performed by the control CPU 710 of the optical disk record regenerative apparatus of drawing 7 . First, in step S1101, in advance of record of AV data from an optical disk 701, the disk identification information in the lead-in groove field 101 is reproduced, and it judges whether the contents which it is going to reproduce now are refreshable in step S1102 in drawing 11 from the classification of the refreshable data currently recorded on disk identification information. When it is NO at step S1102, playback actuation is stopped by step S1112, and regeneration of the AV data concerned is ended. On the other hand, when it is YES at step S1102, in the key management information which reproduced the data which are the sector on which it is step S1103 and key management information was recorded in the key management information field 107 of the lead-in groove field 101, and was reproduced in step S1104, it judges whether key information required for playback of contents is record ending. If it is NO while progressing to step S1106 as it is, when it is YES at step S1104, in step S1105, a descrambling key will be acquired from the key management pin center,large which has managed the key through a communication circuit 711, and it will record on the key management information field 107 of an optical disk 701, and will progress to step S1106.

[0106] Subsequently, at step S1106, control CPU 710 moves the optical head 702 to the user data area of an optical disk 701, controls the record playback control circuit 703, the strange demodulator circuit 704, error detection, and the correction circuit 705, and reproduces AV data. And in step S1107, a descrambling key required for descrambling of sector data is acquired from the descrambling key area 505 shown by the key index contained in the header of the reproduced sector, and the scramble currently performed to the descrambling key is decoded by descrambling by disk identification information at step S1108. Furthermore, in step S1108, it judges whether an error is in a descrambling key by checking the error detection code given to the descrambling key. When it is YES at step S1108, it is regarded as the contents (or contents copied unjustly) which came to hand unjustly, playback actuation is stopped by step S1112, and regeneration of the AV data concerned is ended.

[0107] On the other hand, when it is NO at step S1108, in S1109, the data of contents are descrambled by the descrambling key, and AV data which it descrambled are outputted to the MPEG decoder circuit 708 in step S1110. And after control CPU 710 carries out MPEG expanding of the AV data which it descrambled by controlling the

MPEG decoder circuit 708 and an output circuit 709, D/A conversion of it is carried out to a video signal and an audio signal, and it is outputted to high order devices, such as a TV apparatus and audio equipment. Subsequently, at step S1111, it is judged whether it is termination of playback of contents, and when it is NO, return and the above-mentioned processing are repeated to step S1106. On the other hand, regeneration of the AV data concerned is ended at step S1111 at the time of YES.

[0108] In addition, although it was regarded as the contents which considered that were the contents which came to hand unjustly, for example, were copied unjustly and playback actuation was stopped when an error was detected at step S1109 Like the case where the key is not recorded, by performing processing of step S1105, key information may be acquired from the key management pin center,large which has managed the key, and you may record on the key management information field 107 of an optical disk 701 through a communication circuit 711. Thereby, even if it is copied AV data, it can be made refreshable by a key coming to hand to normal.

[0109] Drawing 12 is a flow chart which shows acquisition processing of the descrambling key performed by the control CPU 710 of the optical disk record regenerative apparatus of drawing 7 . This processing is processing which reproduces a descrambling key from the reproduced key index, and is performed in advance of regeneration of AV data illustrated by drawing 11 .

[0110] In drawing 12 first at step S1201 When it is NO, while judging whether the data of the reproduced sector field are scrambled by scramble control information, and progressing to step S1206, when it is YES A key index is acquired by reproducing the key information currently recorded in the same sector field as the above-mentioned sector field in step S1202. Subsequently After acquiring the descrambling key shown by the above-mentioned key index from the descrambling key area 505 in step S1203, at step S1204 The acquired descrambling key is descrambled using disk identification information, and it judges whether an error has a descrambling key by investigating an error detection code. At step S1204, at the time of YES, playback actuation is stopped by step S1205, and it ends acquisition processing of the descrambling key concerned. On the other hand, when it is NO at step S1204, it progresses to step S1206. When there is no error in the result which disk identification information descrambled about the case where the reproduced sector is not scrambled, or a descrambling key, playback actuation is permitted in step S1206, the data of the reproduced sector are outputted and acquisition processing of the descrambling key concerned is ended.

[0111] As explained above, in the optical disk and optical disk record regenerative apparatus of an operation gestalt concerning this invention, the record and playback

actuation by the user are controlled using the disk identification information only for playbacks created in the disk manufacture phase, and it can do. Furthermore, by scrambling some data using the above-mentioned disk identification information, to the disk with which the physical copy of a user data area was performed, it can reproduce normally and thing prevention can be carried out. Moreover, record of contents and record of a descrambling key can be independently performed by arranging a descrambling key required for descrambling of data to another field with data. For this reason, it can consider as the refreshable condition of contents by recording contents and acquiring a descrambling key if needed at the time of playback of the data of contents for example. Under the present circumstances, it is clear that the unjust utilization by the physical copy can be prevented like the case where it mentions above by scrambling a descrambling key by disk identification information. it -- in addition, even if it is the disk copied unjustly, it can also be made a correctly reproducible optical disk by acquiring the descrambling key scrambled by the disk identification information of the optical disk from a key management pin center,large to a forward type, and recording on an optical disk.

[0112] In addition, although what was already enciphered about the data of contents inputted into an optical disk record regenerative apparatus was explained, the inputted data of contents are enciphered by having the circuit which enciphers contents in an optical disk record regenerative apparatus, and the same effectiveness is acquired by recording on an optical disk.

[0113] Moreover, although the copy between the disks which have different disk identification information by enciphering only a descrambling key required for decode of the enciphered contents using disk identification information was prevented with this operation gestalt, a copy can be similarly prevented by giving encryption which used disk identification information for the contents itself. Furthermore, unjust decode of the contents recorded on the disk can be made more into difficulty by enciphering by using a private key also for disk identification information.

[0114] The optical disk of the operation gestalt concerning <effectiveness of 1st and 2nd operation gestalten> this invention can control the record actuation and the playback actuation of contents of up to the optical disk by the user using the information recorded at the time of manufacture of an optical disk by being recorded on the field only for playbacks which cannot rewrite the disk identification information which performs record actuation to a user data area, and playback actuation for every optical disk.

[0115] When the data enciphered as a key record the disk identification information only for playbacks which is not rewritable on the user data area on an optical disk, even

if it copies the optical disk of the operation gestalt concerning this invention to other record mold optical disks of the user data area by the user, it cannot copy disk identification information but playback of it can be made impossible at the right decode list of data.

[0116] The optical disk of the operation gestalt concerning this invention becomes possible [acquiring independently the descrambling key for solving acquisition and code of the data which need protection of copyrights, such as a film and music,] by being recorded on the sector field to which the enciphered data differ from the descrambling key which solves a code. Furthermore, by enciphering and recording a descrambling key by using disk identification information as a key Even if it copies to other record mold optical disks of the user data area by the user Disk identification information cannot be copied, but playback can be made impossible at the right decode list of data, and playback can be made possible at the right decode list of data by acquiring and recording the descrambling key which enciphered the disk identification information of the optical disk of a copy place as a key.

[0117] It explains referring to a drawing about the encryption contents record and the playback approach of <3rd operation gestalt> Being the 3rd operation gestalt which ranks second and starts this invention. Drawing 16 is the top view showing the data storage area of the optical disk 1101 which is the 3rd operation gestalt concerning this invention.

[0118] In drawing 16 , the record mold optical disk which 1101 is the record medium which can record digital data, and is an optical disk of an erasable type or a postscript mold, the control user data area where 1102 was recorded in the form of the concavo-convex pit where disk information is minute, the user data area where a user records data when 1103 irradiates the light beam of a laser beam at an optical disk, and 1104 are BCA(s) on which Disk ID was recorded. In BCA1104, the disk ID trimming of the record film on the concavo-convex pit where the inner circumference part of the control user data area 1102 is minute is carried out, and it is [disk] descrambling identification information by this by emitting the laser beam of pulse lasers, such as an YAG laser, selectively to the record film so that it may be a long configuration radially and two or more trimming fields 1105 may be formed is recorded.

[0119] Drawing 17 is the wave form chart showing the signal wave form of the regenerative signal 1201 in the BCA regenerative circuit 1401 concerning the 3rd operation gestalt, and the playback binary-ized signal 1207, and drawing 18 is the block diagram showing the configuration of the BCA regenerative circuit 1401 concerning the 3rd operation gestalt. In drawing 17 , the regenerative signal 1201 when reproducing

the data of BCA1104 is shown. For an optical pickup and 1302, as for a low pass filter (LPF) and 1304, in drawing 18 , pre amplifier and 1303 are [1301 / a binary-ized circuit and 1305] demodulator circuits.

[0120] In drawing 18 , after the laser beam outputted from an optical pickup 1301 irradiates BCA1104 of an optical disk 1101 and photo electric translation of the reflected light is carried out by the optical pickup 1301, the electrical signal after photo electric translation is amplified by pre amplifier 1302, and a regenerative signal 1201 is acquired. Here, the regenerative signal 1201 of drawing 17 is a signal which has the level according to the concavo-convex pit of the control user data area 1102, and is a trimming part which record film was removed by trimming processing according [1202, 1203, and 1204] to a pulse laser, and lacks the signal by the concavo-convex pit in this regenerative signal 1201. This trimming processing is performed by the manufacturer of an optical disk.

[0121] If return explanation is given at drawing 18 , a regenerative signal 1201 will be inputted into the binary-ized circuit 1304, after being inputted into a low pass filter 1303 and removing the modulating signal by the concavo-convex pit. The regenerative signal inputted into the binary-ized circuit 1304 is made binary not using the usual slice level 1205 which makes binary the signal of the control user data area 1102 but using the slice level 1206 which is level lower enough than slice level 1205, and the playback binary-ized signal 1207 is acquired. It restores to the playback binary-ized signal 1207 outputted from the binary-ized circuit 1304 in a demodulator circuit 1305, and the disk ID signal 1306 is acquired.

[0122] As explained above, management of an optical disk is easily realizable by adding the disk identification information which identifies an optical disk. Moreover, it can prevent that the information which identifies the optical disk in BCA1104 is altered easily by recording BCA1104 on a concavo-convex pit. Furthermore, when the control user data area 1102 and BCA1104 of drawing 16 adjoin In case the data of the control user data area 1102 are reproduced, the data of BCA1104 can also be reproduced continuously. Or since the data of the control user data area 1102 can be continued and it can reproduce in case the data of BCA1104 are reproduced For example, it becomes possible to bring forward the processing for the information on BCA1104 for CPU identifying an optical disk promptly coming to hand, in case an optical disk is started, and recording the enciphered contents.

[0123] In addition, although BCA1104 of this operation gestalt is formed by trimming the record film on the concavo-convex pit of the inner circumference part of the control user data area 1102, the record film which constitutes the record form optical disk

which is an optical disk of an erasable type or a postscript mold tends to be influenced by heat to the reflective film in the optical disk only for playbacks. By trimming the inner circumference part of the control user data area 1102, the user data area 1103 can be protected from the heat generated in the case of trimming compared with the case where a periphery part is trimmed. Moreover, BCA1104 is formed in the inner circumference side of the control user data area 1102 because the margin in case the path of the spot of the beam of a laser beam changes with the instability of a focus servo circuit is taken into consideration.

[0124] In addition, the data currently recorded on BCA1104 in front of trimming may be recorded on the control user data area 1102. By being recorded also on the control user data area 1102, even if the data currently recorded on BCA1104 perform trimming, they can protect the above-mentioned data of the control user data area 1102. Furthermore, when the data currently recorded on BCA1104 are continuously recorded repeatedly from BCA1104 to the control user data area 1102, the location of BCA1104 can be expected by finding the above-mentioned data of the control user data area 1102.

[0125] Subsequently, the procedure which records the contents enciphered by Disk ID through the network by the optical disk 1101 which has the above BCA1104 is described. In the 3rd thru/or 5th operation gestalt, a network means communication networks, such as the Internet, a dial-up line, or a dedicated line. Drawing 19 shows the equipment configuration which records encryption contents to the record mold optical disk 1101 which is the block diagram showing the optical disk record playback structure of a system concerning the 3rd operation gestalt, and is an optical disk of the erasable type which has the above BCA1104, or a postscript mold.

[0126] In drawing 19 , an optical disk record regeneration system is equipped with the optical disk record regenerative apparatus 1410 each other connected through the networks 1405, such as the Internet, and the encryption section 1406, and is constituted. The optical disk record regenerative apparatus 1410 is equipped with an optical pickup 1301, the BCA regenerative circuit 1401, the Internet 403, a record circuit 1411, the data playback section 1412, and the code decoder 1413. Moreover, the encryption section 1406 is equipped with an interface 1404, the contents memory 1407, and the encryption encoder 1408.

[0127] First, the laser beam outputted from an optical pickup 1301 irradiates BCA1104 of the RAM mold optical disk 1101, and after photo electric translation of the reflected light is carried out by the optical pickup 1301, the regenerative signal by which photo electric translation was carried out is inputted into the BCA regenerative circuit 1401. The BCA regenerative circuit 1401 reproduces the disk ID signal 1402 in BCA based on

the inputted regenerative signal, and it is sent to the encryption encoder 1408 of the encryption section 1406 through interfaces 1403 and 1404 and a network 1405 while it outputs the reproduced disk ID signal 1402 to the code decoder 1413. The encryption encoder 1408 enciphers the data of the contents concerned, or performs the scramble for image voice so that the disk ID signal 1402 of the optical disk 1101 with which the data of the contents in the contents memory 1407 are recorded may serve as a decode key which solves a code.

[0128] In addition, with this operation gestalt, about encryption processing, if it enciphers using the disk ID signal 1402 as a cryptographic key, even if it will express contents 1407, they are made into the same semantics. Moreover, in this operation gestalt, encryption and a decryption are considered with the relation between a lock and a key, and it considers shutting the above-mentioned lock with the above-mentioned key as encryption, and considers opening the above-mentioned lock with the above-mentioned key as a decryption. Therefore, the key for decrypting with the key for enciphering, although actual operations differ by encryption and decryption presupposes that it is the same. In addition, contents 1407 are set to C, the disk ID signal 1402 is set to BCAS, the enciphered contents 1409 are set to C [BCAS], and the operation of encryption processing is expressed with * and written like a degree type.

[0129]

[Equation 1] C*BCAS=C[BCAS]

[0130] The contents 1409 enciphered by the encryption section 1406 are sent to the record circuit 1411 of the record regenerative apparatus 1410 through interfaces 1403 and 1404 and a network 1405. A record circuit 1411 records the data of contents on an optical disk 1101 by predetermined carrying out digital modulation of the data of contents inputted, carrying out intensity modulation of the laser beam from an optical pickup 1301 according to the data by which digital modulation was carried out, and irradiating an optical disk 1101.

[0131] Next, when reproducing the above-mentioned contents which were enciphered by the optical disk 1101 and recorded on it, after the laser beam outputted from an optical pickup 1301 irradiates the field where the above-mentioned encryption contents of the user data area 1103 were recorded and photo electric translation of the reflected light is carried out by the optical pickup 1301, the regenerative signal by which photo electric translation was carried out is inputted into the data playback section 1412. The data playback section 1412 carries out A/D conversion of the inputted regenerative signal to digital data, and outputs it to the code decoder 1413. On the other hand, after the laser beam from an optical pickup 1301 irradiates BCA1104 of an optical disk 1101 and photo

electric translation of the reflected light is carried out by the optical pickup 1301, the regenerative signal by which photo electric translation was carried out is inputted into the BCA regenerative circuit 1401. The BCA regenerative circuit 1401 carries out A/D conversion of the inputted regenerative signal, generates the disk ID signal 1402, and outputs the disk ID signal concerned to the code decoder 1413.

[0132] The code decoder 1413 decodes the data of the enciphered contents, using the inputted disk ID signal 1402 as a key. The key for decoding the encryption contents currently recorded on the optical disk 1101, when contents are recorded on normal by the optical disk 1101 at this time is the disk ID signal 1402 of an optical disk 1101, and the disk ID signal 1402 outputted from the BCA regenerative circuit 1401 at the time of playback is also a disk ID signal (BCAS) of an optical disk 1101. Therefore, the contents which it decoded or descrambled are outputted as an output signal 1414 from the code decoder 1413. In addition, if the operation of decryption processing is made into #, it will be written like a degree type.

[0133]

[Equation 2] C[BCAS] #BCAS=C [0134] Here, when the data of contents are image data, the data of an MPEG signal are elongated and the data of a picture signal are obtained.

[0135] As explained above, the encryption in this operation gestalt is using Disk ID as the key, and since only one piece exists corresponding to the optical disk of one sheet, Disk ID is effective in the same encryption contents being recordable only on the optical disk concerned of one sheet. That is, when it is going to copy to another optical disk with an another disk ID called ID2 in the above-mentioned contents 1407 and is going to reproduce from the optical disk with a disk ID called ID1 of normal, ID2 is outputted as a disk ID signal 1402 from the BCA regenerative circuit 401. However, since it is enciphered by the disk ID signal of ID1, encryption contents are the code decoders 1413 and cannot decode encryption contents.

[0136] In addition, the encryption encoder 1408 may be the gestalt of the IC card which is in a record regenerative-apparatus side not to the supply origin of contents but to a network, and carried the encryption encoder. Moreover, since it is enciphered by Disk ID, the above-mentioned optical disk 1101 can be reproduced with the optical disk record regenerative apparatus of the arbitration which has the BCA regenerative circuit 1401 and the code decoder 1413.

[0137] It explains referring to a drawing about the encryption contents record approach which <4th operation gestalt> Is the 4th operation gestalt which ranks second and starts this invention. Drawing 20 is the block diagram showing the optical disk record playback structure of a system which is the 4th operation gestalt concerning this

invention, and shows the equipment configuration which records encryption contents to the record mold optical disk which is the erasable type or write once optical disk which has BCA. In addition, in explanation of the 4th operation gestalt, the 3rd operation gestalt and a common part simplify the explanation.

[0138] In drawing 20 , the optical disk record regeneration system concerning the 4th operation gestalt is equipped with CATV firm equipment 1501, key issuance pin center,large equipment 1507, the CATV decoder 1506, the optical disk record regenerative apparatus 1514, and TV apparatus 1530, and is constituted. Here, CATV firm equipment 1501 is equipped with the contents memory 1502 which stores the data of contents, such as film software, the 1st cryptographic key memory 1503 which stores the 1st cryptographic key, and the 1st encryption encoder 1504. Moreover, key issuance pin center,large equipment 1507 is equipped with control section 1507a which controls actuation of the equipment 1507, the time limit information memory 1510 which stores time limit information, and the record authorization code memory 1511 which stores a record authorization code. Furthermore, the CATV decoder 1506 is equipped with the system ID memory 1508 which stores the system ID of the CATV decoder 1506, the 1st code decoder 1513, the 2nd encryption encoder 1516, and the firm recognition signal memory 1523 in IC card 1522. Furthermore, the optical disk record regenerative apparatus 1514 is equipped with a record circuit 1518, the data playback section 1519, the BCA regenerative circuit 1521, the 2nd code decoder 1520, and the firm recognition signal memory 1526 in IC card 1524.

[0139] First, by enciphering the data of the contents in the contents memory 1502, such as film software, using the 1st cryptographic key 1503, the 1st encryption encoder 1504 of CATV firm equipment 1501 generates the 1st encryption contents 1505, and transmits the generated 1st encryption contents 1505 to the 1st encryption decoder 1513 of each user's CATV decoder 1506 through a network. Here, if the data in the contents memory 1502 are set to C, the 1st cryptographic key 1503 is set to FK and the 1st encryption contents 1505 are set to C [FK], it will be written like a degree type.

[0140]

[Equation 3] C*FK=C[FK]

[0141] The CATV decoder 1506 transmits the title code 1509 which was beforehand given to the above-mentioned contents to perform record to the system ID of the CATV decoder 1506 concerned in the system ID memory 1508, and viewing and listening or the RAM mold optical disk 1101, for example, was inputted using the keyboard (not shown) of the CATV decoder 1506 concerned to key issuance pin center,large equipment 1507 through a network. Here, the title code 1509 may be inputted by choosing

according to the screen of TV, may be directly inputted from a keyboard, and may be inputted from a remote controller etc. Therefore, the user may receive the title code 1509 uniquely, it may be sent to the CATV decoder 1506 with the 1st encryption contents 1505, and may be beforehand sent with the gestalt of program advice etc. at time of day when the 1st encryption contents 1505 are another.

[0142] a key -- issuance -- a pin center,large -- equipment -- 1507 -- a control section -- 1507 -- a -- CATV -- a decoder -- 1506 -- a system ID -- the above -- contents -- a title -- a code -- 1509 -- being based -- a time limit -- information -- memory -- 1510 -- inside -- a time limit -- information -- record -- an authorization code -- memory -- 1511 -- inside -- record -- an authorization code -- referring to -- these -- corresponding -- a key -- (-- K --) -- 1512 -- a record authorization code and a time limit code -- the 1st code decoder 1513 of the CATV decoder 1506 -- receiving -- a network -- minding -- transmitting . In addition, the case where change time of day and multiple-times broadcast of the same contents is carried out using time limit information is distinguishable. Here, when set the 1st decode key to FK, set the system ID of the CATV decoder 1506 to DID, time limit information is set to TIME, a record authorization code is set to COPY and the title code 1509 of contents is set to T, the key (K) is filling the relation of a degree type.

[0143]

[Equation 4] FK=K*T*DID*TIME*COPY [0144] In addition, it is determined whether the record authorization code in the record authorization code memory 1511 permits both viewing and listening and record for whether do the contents which CATV firm equipment 1501 broadcasts judge a new work article or the old work and only viewing and listening is permitted.

[0145] CATV -- a decoder -- 1506 -- the -- one -- a code -- a decoder -- 1513 -- the -- one -- decode -- a key -- (-- FK --) -- a key -- (-- K --) -- 1512 -- the above -- contents -- a title -- a code -- 1509 -- a system ID -- record -- an authorization code -- a time limit -- information -- a **** -- relation -- filling -- **** -- and -- a clock -- a circuit -- 1527 -- from -- outputting -- having -- current time -- information -- being concerned -- a time limit -- information -- conditions -- filling -- **** -- if -- the 1st encryption contents 1505 -- decoding . Here, when the contents by which encryption was carried out [above-mentioned] are picture signals, the picture signal which it descrambled is outputted to TV apparatus 1530, and can view from the 1st encryption decoder 1513 and listen. Here, decryption processing of the 1st encryption decoder 1513 is expressed with a degree type.

[0146]

[Equation 5]

C[FK]#(K*T*DID*TIME*COPY)

= C[FK] #FK=C [0147] In addition, when a record authorization code permits only viewing and listening, it cannot record on an optical disk 1101, but since it can record when permitting both viewing and listening and record, this approach is explained below.

[0148] The BCA regenerative circuit 1521 of the optical disk record regenerative apparatus 1514 reproduces the data of BCA1104 of an optical disk 1101, acquires the disk ID signal 1515, and outputs the disk ID signal concerned to the 2nd encryption encoder 1516 of the CATV decoder 1506. By enciphering the data of the contents outputted from the 1st code decoder 1513, using the disk ID signal 1515 as the 2nd cryptographic key, the 2nd encryption encoder 1516 of the CATV decoder 1506 generates the 2nd encryption contents 1517, and transmits them to the record circuit 1518 of the optical disk record regenerative apparatus 1514. In addition, the above-mentioned encryption of the 2nd code decoder 1516 is restricted to the time amount to which the 1st encryption contents are decoded and outputted from the 1st code decoder 1513. Here, if the contents which are the output signals of the 1st code decoder 1513 are set to C, the disk ID signal 1515 which is the 2nd cryptographic key is set to BCAS and the 2nd encryption contents 1517 are set to C [BCAS], it will be written like a degree type.

[0149]

[Equation 6] C*BCAS=C[BCAS]

[0150] A record circuit 1518 becomes irregular, for example by 8/16 well-known modulation technique, and the 2nd encryption contents 1517 sent to the record circuit 1518 of the optical disk record regenerative apparatus 1514 are recorded on the user data area 1103 of an optical disk 1101 by the optical pickup (not shown). In case the above-mentioned contents which were enciphered by the optical disk 1101 and recorded on it are reproduced, the laser beam outputted from an optical pickup irradiates the field where the contents by which encryption of the optical disk 1101 was carried out [above-mentioned] are recorded, and the reflected light carries out incidence to an optical pickup. The above-mentioned optical pickup carries out photo electric translation of the reflected light which carries out incidence, the regenerative signal by which photo electric translation was carried out is outputted to the data playback section 1519, and the data playback section 1519 carries out A/D conversion of the inputted regenerative signal to a digital regenerative signal, and outputs it to the 2nd code decoder 1520.

[0151] On the other hand, the laser beam outputted from an optical pickup irradiates

BCA1104 of an optical disk 1101, and the reflected light carries out incidence to an optical pickup. The above-mentioned optical pickup carries out photo electric translation of the reflected light which carries out incidence, and outputs the regenerative signal by which photo electric translation was carried out to the BCA regenerative circuit 1521. The BCA regenerative circuit 1521 generates the disk ID signal 1515 based on the inputted regenerative signal, and outputs it to the 2nd code decoder 1520. Answering this, the 2nd code decoder 1520 decodes the reproduced encryption contents which are outputted from the data playback section 1519, using the inputted disk ID signal 1515 as a key. Since the key for decoding the encryption contents currently recorded on the optical disk 1101 is the disk ID of an optical disk 1101 and the disk ID signal outputted from the BCA regenerative circuit 1521 is also a disk ID signal (BCAS) of an optical disk 1101 when contents are recorded on normal by the optical disk 1101 at this time, the 2nd code decoder 1520 can perform decode processing normally. Therefore, the data of the contents which it decoded or descrambled are outputted as an output signal 1525 from the 2nd code decoder 1520. Here, decryption processing of the 2nd code decoder 1520 can be written by the degree type, and when contents are picture signals, the 2nd code decoder 1520 elongates for example, an MPEG signal, and reproduces and outputs the original picture signal.

[0152]

[Equation 7] C[BCAS] #BCAS=C [0153] Moreover, since it is enciphered only by the disk ID signal (BCAS) 1515, the above-mentioned optical disk 1101 can be reproduced with the optical disk record regenerative apparatus of the arbitration which has the BCA regenerative circuit 1521 and the 2nd code decoder 1520. In addition, although it explained enciphering with the code encoders 1504 and 1516 and decrypting by the code decoders 1513 and 1520, the program of cryptographic algorithm and a decode algorithm may be constituted so that encryption and a decryption may be performed in preparation for the program performed by each equipments 1501 and 1506 and CPU which is a control section in 1514.

[0154] In addition, in this operation gestalt, although the 2nd encryption encoder 1516 of the CATV decoder 1506 enciphered contents, using the disk ID signal 1515 as the 2nd cryptographic key, contents may be enciphered as follows. For example, the CATV decoder 1506 may be equipped with IC card 1522 prepared every CATV firm equipment 1501, it may use as the 2nd cryptographic key combining the firm recognition signal currently recorded in the firm recognition signal memory 1523 of IC card 1522, and the disk ID signal (BCAS) reproduced by the BCA regenerative circuit 1521, and contents may be enciphered with the 2nd encryption encoder 1516. Here, when set to C the

contents which are the output signals of the 1st code decoder 1513, the disk ID signal 1515 which is the 1st cryptographic key [2nd] is set to BCAS, the firm recognition signal 1523 which is the 2nd cryptographic key [2nd] is set to CK and the 2nd encryption contents 1517 are set to C [BCAS, CK], encryption processing of the 2nd encryption encoder 1516 is written like a degree type.

[0155]

[Equation 8] C*BCAS*CK=C[BCAS,CK]

[0156] Next, in case the contents enciphered and recorded on the optical disk 1101 are reproduced, the laser beam outputted from an optical pickup irradiates the field where the contents by which encryption of the optical disk 1101 was carried out [above-mentioned] are recorded, and the reflected light carries out incidence to an optical pickup. An optical pickup carries out photo electric translation of the reflected light by which incidence is carried out to a regenerative signal, and outputs it to the data playback section 1519. The data playback section 1519 carries out A/D conversion of the regenerative signal inputted to a digital regenerative signal, and outputs it to the 2nd code decoder 1520. On the other hand, the laser beam outputted from an optical pickup irradiates BCA1104 of an optical disk 1101, and the reflected light carries out incidence to an optical pickup. An optical pickup carries out photo electric translation of the reflected light by which incidence is carried out to a regenerative signal, and outputs it to the BCA regenerative circuit 1521. The BCA regenerative circuit 1521 reproduces the disk ID signal 1515 based on the regenerative signal inputted, and outputs the disk ID signal 1515 to the 2nd encryption encoder 1516 and the 2nd code decoder 1520.

[0157] Furthermore, the firm recognition signal in the firm recognition signal memory 1526 of IC card 1524 with which the optical disk record regenerative apparatus 1514 was equipped is inputted into the 2nd code decoder 1520. In addition, the firm recognition signal concerned may be recorded on the memory (not shown) which does not need to be recorded in the firm recognition signal memory 1526 of IC card 1524, for example, was connected to CPU whose firm recognition signal is the control section of the optical disk record regenerative apparatus 1514 at the time of install of the record program of the optical disk record regenerative apparatus 1514. Instead, a firm recognition signal may be inputted using the keyboard (not shown) of the optical disk record regenerative apparatus 1514.

[0158] The 2nd code decoder 1520 decodes the enciphered contents, using the inputted disk ID signal 1515 and a firm recognition signal as a decode key. At this time, it contracts to the specific CATV firm and the specific forward type in which the user of

the CATV decoder 1506 has CATV firm equipment 1502. When contents 1502 are recorded on normal by the optical disk 1101 The 1st decode key of the encryption contents which are enciphered by the optical disk 1101 and recorded on it It is the disk ID signal (BCAS) of the optical disk 1101 which it is just going to play, and the 2nd decode key is a firm recognition signal in the firm recognition signal memory 1526 of IC card 1524 offered from the CATV firm which contracted (CK). Therefore, the output signal 1525 of the contents which it decoded or descrambled is outputted from the 2nd code decoder 1520. Here, decryption processing of the 2nd code decoder 1520 is written like a degree type, when contents are picture signals, an MPEG signal is elongated by the 2nd code decoder 1520, and the output signal 1525 of a picture signal is outputted.

[0159]

[Equation 9]

C[BCAS, CK] #(BCAS*CK) =C [0160] Moreover, since it is enciphered with the disk ID signal 1515 and the firm recognition signal, the contents of the above-mentioned optical disk 1101 can be reproduced with the optical disk record regenerative apparatus of the BCA regenerative circuit 1521 and the arbitration which has the 2nd code decoder 1520, if the agreement is contracted with the CATV firm of the offer origin of the above-mentioned contents. On the contrary, if it has not contracted with the above-mentioned CATV firm, since a firm recognition signal cannot come to hand, contents cannot be reproduced but differentiation with a user [finishing / an agreement] is enabled.

[0161] Moreover, with this operation gestalt, since each user enciphers the optical disk record regenerative apparatus 1514 to a disk ID signal for delivery, image data, etc. to the CATV decoder 1506 of a house, CATV firm equipment 1501 does not need to change the encryption contents distributed to each user according to an individual, can simplify the system at the time of broadcast, is low cost and can offer the same contents as the viewer of a large quantity. Furthermore, according to this operation gestalt, record is permissible to one RAM mold optical disk for every user which has the CATV decoder 1506.

[0162] In addition, although this operation gestalt explained the case where contents were broadcast from the head end of cable television, the same is said of broadcast by the electric wave.

[0163] It explains referring to a drawing to a <operation gestalt of ** 5th> pan about the encryption contents record and the playback approach of being the 5th operation gestalt concerning this invention. Drawing 21 is the top view showing the data storage area of the optical disk 1601 which is the 5th operation gestalt concerning this invention, and

drawing 22 is the block diagram showing the optical disk record playback structure of a system concerning the 5th operation gestalt. In addition, in the 5th operation gestalt, the 3rd and 4th operation gestalten and a common part simplify the explanation.

[0164] In drawing 21 , when the record mold optical disk whose 1601 is an erasable type or a write once optical disk, the control user data area where 1602 was recorded in the form of the concavo-convex pit in disk information, and 1603 irradiate the light beam of a laser beam at an optical disk, a user data area for a user to record data and 1604 are BCA(s) on which Disk ID was recorded.

[0165] In BCA1604, by carrying out trimming of the record film on the concavo-convex pit of the inner circumference part of the control user data area 1602 by pulse lasers, such as an YAG laser, selectively, radially, it is a long configuration and two or more trimming fields 1606 are formed. In addition, trimming is performed by the disk manufacturer. Moreover, management of an optical disk is easily realizable by adding Disk ID to the data recorded on BCA1604. Furthermore, it can prevent that the information which was recorded on BCA1604 and which identifies an optical disk is altered easily by recording the data of BCA1604 on a concavo-convex pit.

[0166] Furthermore, when BCA1604 adjoins the control user data area 1602 In case the data of the control user data area 1602 are reproduced, the data of BCA1604 can also be reproduced continuously. Or since the data of the control user data area 1602 can be continued and it can reproduce in case the data of BCA1604 are reproduced For example, it becomes possible to bring forward the processing for the information on BCA1604 for CPU identifying a disk promptly coming to hand, in case an optical disk is started, and recording the enciphered contents.

[0167] In addition, although BCA1604 of this operation gestalt is formed by trimming the record film on the concavo-convex pit of the inner circumference part of the control user data area 1602, the record film which constitutes the record mold optical disk which is an erasable type or a write once optical disk tends to be influenced by heat to the reflective film in the optical disk only for playbacks. By trimming the inner circumference part of the control user data area 602, the record data of the user data area 1603 can be protected from the heat generated in the case of trimming compared with the case where a periphery part is trimmed. Moreover, BCA1604 is formed in the inner circumference side of the control user data area 1602 because the margin in case the path of the spot of the beam of a laser beam changes with the instability of a focus servo circuit is taken into consideration. In addition, the data currently recorded on BCA1604 in front of trimming may be recorded on the control user data area 1602. By being recorded also on the control user data area 1602, even if the data currently

recorded on BCA1604 perform trimming, they can protect the above-mentioned data of the control user data area 1602.

[0168] Furthermore, when the above-mentioned data are continuously recorded repeatedly from BCA1604 to the control user data area 1602, the location of BCA1604 can be expected by finding the above-mentioned data of the control user data area 1602. Moreover, the data of the key information record section 1605 are recorded by irradiating a light beam as well as the user data area 1603.

[0169] Like this operation gestalt, when the control user data area 1602 and the key information record section 1605 adjoin In case the data of the control user data area 1602 are reproduced, the data of the key information record section 1605 can also be reproduced continuously. Or since the data of the control user data area 1602 can be continued and it can reproduce in case the data of the key information record section 1605 are reproduced For example, it becomes possible to bring forward the processing for the information on BCA1604 for CPU identifying a disk promptly coming to hand, in case an optical disk is started, and reproducing the enciphered contents.

[0170] In drawing 22 , the optical disk record regeneration system concerning the 5th operation gestalt is equipped with CATV firm equipment 1701, key issuance pin center,large equipment 1707, the CATV decoder 1706, the optical disk record regenerative apparatus 1714, and TV apparatus 1730, and is constituted. Here, CATV firm equipment 1701 is equipped with the contents memory 1702 which stores contents, such as film software, the 1st cryptographic key memory 1703 which stores the 1st cryptographic key, and the 1st encryption encoder 1704. Moreover, the CATV decoder 1706 is equipped with the clock circuit 1725 which outputs the system ID memory 1708, the 1st code decoder 1713, and current time information. Furthermore, key issuance pin center,large equipment 1707 is equipped with control-section 1707a which controls actuation of the equipment 1707 concerned, and the time limit information memory 1710 which stores time limit information. Furthermore, the optical disk record regenerative apparatus 1714 is equipped with a record circuit 1717, the key information record circuit 1719, the BCA regenerative circuit 1720, the data playback section 1721, the 2nd code decoder 1722, and the key information playback section 1723.

[0171] First, by enciphering the data of contents, such as film software in the contents memory 1702, using the 1st cryptographic key 1703, the 1st encryption encoder 1704 of CATV firm equipment 1701 generates the 1st encryption contents 1705, and transmits them to the 1st code decoder 1713 of each user's CATV decoder 1706 through a network. Here, if the contents in the contents memory 1702 are set to C, the 1st cryptographic key in the 1st cryptographic key memory 1703 is set to FK and the 1st encryption

contents 1705 are set to C [FK], it will be written like a degree type.
[0172]
[Equation 10] C*FK=C[FK]
[0173] The CATV decoder 1706 transmits the system ID in the system ID memory 1708 of the CATV decoder 1706, and the title code 1709 of the above-mentioned contents inputted using the keyboard (not shown) to view and listen through a network to control-section 1707a of key issuance pin center,large equipment 1707. In addition, the above-mentioned title code may be inputted by choosing according to the screen of TV apparatus 1730, may be inputted from a direct keyboard, and may be inputted from a remote controller etc. Therefore, the user may receive the title code uniquely, it may be sent to the CATV decoder 1706 with the 1st encryption contents, and may be beforehand sent at time of day different from the 1st encryption contents with the gestalt of program advice etc.
[0174] a key -- issuance -- a pin center,large -- equipment -- 1707 -- a control section -- 1707 -- a -- CATV -- a decoder -- 1706 -- a system ID -- the above -- contents -- a title -- a code -- being based -- a time limit -- information -- memory -- 1710 -- inside -- corresponding -- a time limit -- information -- referring to -- corresponding -- a key -- (-- K --) -- 1712 -- generating -- the 1st code decoder 1713 of the CATV decoder 1706 -- a network -- minding -- transmitting . In addition, the case where change time of day and multiple-times broadcast of the same contents is carried out using time limit information is distinguishable. Here, when set the 1st decode key to FK, the system ID of the CATV decoder 1706 is set to DID, time limit information is set to TIME and the title code of contents is set to T, the key (K) 1712 is filling the relation of a degree type.
[0175]
[Equation 11] FK=K*T*DID*TIME [0176] the -- one -- a code -- a decoder -- 1713 -- the -- one -- decode -- a key -- (-- FK --) -- a key -- issuance -- a pin center,large -- equipment -- 1707 -- from -- transmitting -- having -- the above -- a key -- (-- K --) -- 1712 -- the above -- contents -- a title -- a code -- a system ID -- a time limit -- information -- a **** -- relation -- filling -- **** -- and -- a time limit -- information -- a clock -- a circuit -- 1725 -- from -- current time -- information -- conditions -- filling -- **** -- if -- the 1st encryption contents 1705 -- it can decode -- . When the 1st encryption contents 1705 are picture signals, the picture signal which it descrambled is outputted to TV apparatus 1730 from the 1st encryption decoder 1713, and a user can view [here,] and listen to contents with TV apparatus 1730. Here, decryption processing of the 1st encryption decoder 1713 is written like a degree type.
[0177]

[Equation 12]

C[FK]#(K*T*DID*TIME

= C[FK] #FK=C [0178] Next, how to record the above-mentioned contents on an optical disk 1601 is explained. In case contents are recorded on an optical disk 1601, the 1st encryption contents 1705 which are not decrypted by the CATV decoder 1706 are transmitted to the record circuit 1717 of the optical disk record regenerative apparatus 1714 from the 1st encryption encoder 1704 of CATV firm equipment 1701. A record circuit 1717 carries out digital modulation of the data of the received 1st encryption contents 1705, for example using modulation techniques, such as 8/16 well-known modulation technique, and the digital data after a modulation is recorded on an optical disk 1601 by the optical pickup (not shown). Therefore, in order to reproduce the above-mentioned contents which were enciphered by the optical disk 1601 and recorded on it, it is necessary to decode the 1st encryption contents 1705.

[0179] The optical disk record regenerative apparatus 1714 transmits the disk ID signal 1715 of an optical disk 1601 reproduced by the BCA regenerative circuit 1720, and the title code 1716 of the above-mentioned contents inputted using the keyboard (not shown) to reproduce through a network to control-section 1707a of key issuance pin center,large equipment 1707. In addition, in case the timing which sends Disk ID accesses with key issuance pin center,large equipment 1707, it may be sent, or it may be sent together with a title code in the case of viewing and listening.

[0180] Moreover, as the transmitting approach of Disk ID, as shown in drawing 22 , BCA1604 of an optical disk 1601 is reproduced, and although the approach of sending the output signal of the BCA regenerative circuit 1720 to direct key issuance pin center,large equipment 1707 is indicated above, this invention may use not only this but the following approach. For example, before access with the key issuance pin center,large equipments 1707 at the time of disk starting etc., the data of BCA1604 are reproduced, it is kept in the memory (not shown) of the optical disk record regenerative apparatus 1714 or the CATV decoder 1706, and you may transmit to control-section 1707a of key issuance pin center,large equipment 1707 to the above-mentioned timing. Furthermore, when you may input from a keyboard when Disk ID can recognize also visually with the gestalt of a label etc., and the label has become a bar code, it is as a bar code reader to reading.

[0181] a key -- issuance -- a pin center,large -- equipment -- 1707 -- a control section -- 1707 -- a -- an optical disk -- 1601 -- a disk -- ID -- a signal -- 1715 -- and -- contents -- a title -- a code -- 1716 -- corresponding -- a key -- (-- DK --) -- 1718 -- generating -- the key information record circuit 1719 of the optical disk record regenerative apparatus 1714 --

transmitting . Here, when setting the 1st decode key to FK, setting the disk ID signal 1715 of an optical disk 1601 to BCAS and setting the title code 1716 of contents to T, the key (DK) is filling the relation of a degree type.

[0182]

[Equation 13] FK=DK*BCA*T [0183] Digital modulation of the key (DK) inputted into the key information record circuit 1719 of the optical disk record regenerative apparatus 1714 is carried out, for example using modulation techniques, such as 8/16 well-known modulation technique, and the digital data after a modulation is recorded on the key information record section 1605 of an optical disk 1601 by the optical pickup (not shown). In addition, as for a key (DK), two or more same keys may be recorded on the key information record section 1605. Contents can be decoded, if a key (DK) can be protected and the data of any one key (DK) can be reproduced, when the record film of the key information record section 1605 deteriorated by recording two or more same keys, or when a blemish is attached to an optical disk 1601.

[0184] Moreover, with this operation gestalt, although the key information record section 1605 is established in the inner circumference side of the user data area 1603, it may be in the periphery side of the user data area 1603, and may be established in both by the side of inner circumference and a periphery. By being prepared in a periphery side, it becomes possible to record more keys (DK). Moreover, even when it becomes impossible to reproduce one key information record section by preparing two or more key information record sections dispersedly, a key (DK) can be protected by other key information record sections.

[0185] On the other hand, the laser beam outputted from an optical pickup irradiates the field where the above-mentioned contents of an optical disk 1601 were recorded, and the reflected light carries out incidence to an optical pickup. An optical pickup carries out photo electric translation of the reflected light which carries out incidence, and outputs the regenerative signal by which photo electric translation was carried out to the data playback section 1721. This is answered, and the data playback section 1721 carries out A/D conversion of the inputted regenerative signal to encryption digital data, and outputs it to the 2nd code decoder 1722. Furthermore, the laser beam outputted from an optical pickup irradiates BCA604 of an optical disk 1601, and the reflected light carries out incidence to an optical pickup. An optical pickup carries out photo electric translation of the reflected light which carries out incidence, and outputs the regenerative signal by which photo electric translation was carried out to the BCA regenerative circuit 1720. This is answered, and the BCA regenerative circuit 1720 reproduces the disk ID signal 1715 based on the regenerative signal inputted, and

outputs it to the code decoder 1722. Furthermore, the laser beam outputted from an optical pickup irradiates the key information record section 1605 of an optical disk 1601, and the reflected light carries out incidence to an optical pickup. An optical pickup carries out photo electric translation of the reflected light which carries out incidence, and outputs a regenerative signal to the key information playback section 1723, and this is answered, and the key information playback section 1723 generates the data of a key (DK) based on the regenerative signal inputted, and outputs them to the 2nd code decoder 1722.

[0186] In addition, in case it accesses to key issuance pin center,large equipment 1707 and contents are reproduced immediately, before the key information record circuit 1719 records a key (DK) on the key information record section 1605, it may be directly inputted into the 2nd code decoder 1722. By doing in this way, time amount until it starts playback can be shortened. The code decoder 1722 decodes the enciphered contents using the decode key which consists of an inputted disk ID signal 1715, and a key (DK) and the title code 1716 of the above-mentioned contents. Decryption processing of the 2nd code decoder 1722 is expressed with a degree type. When contents are picture signals, an MPEG signal is elongated and the output signal 1724 of a picture signal is outputted from the 2nd code decoder 1722.

[0187]

[Equation 14]

C[FK]#(DK*BCA*T)

= C[FK] #FK=C [0188] In this operation gestalt, when receiving a key signal from control-section 1707a of key issuance pin center,large equipment 1707, supposing it is charged, when viewing and listening, and when reproducing the contents recorded on the optical disk 1601 for the first time, it will be charged independently, and will not be charged only by recording on an optical disk 1601. Therefore, it can collect to both records and the amount of money charged can be made cheap for the user who does not need to record on an optical disk 1601 to the case to viewing and listening and an optical disk 1601 where it charges although he wants to carry out viewing and listening, and the user who do not need to view and listen when broadcast although he wants to record on an optical disk 1601. Moreover, after viewing and listening, since it is not charged only by recording on an optical disk 1601, a user can determine whether receive the key for playing an optical disk 1601, in order to view and listen again. in the above operation gestalt, although the key (DK) use the approach of receive through a network from control section 1707a of key issuance pin center,large equipment 1707, by tell the title and disk ID number of not only this but contents orally by telephone etc., this invention

may be receive orally and it may input it from a keyboard.

[0189] Next, the case where the optical disk 1601 with which the key (DK) was recorded on the key information record section 1605 is played after access termination with key issuance pin center,large equipment 1707 is explained. First, the laser beam outputted from an optical pickup irradiates the field where the above-mentioned contents of an optical disk 1601 were recorded, and the reflected light is inputted into the data playback section 1721 through the optical pickup which performs photo electric translation. Answering this, the data playback section 1721 outputs the data of the enciphered contents to the 2nd code decoder 1722. On the other hand, the laser beam outputted from an optical pickup irradiates BCA1604 of an optical disk 1601, and is inputted into the BCA regenerative circuit 1720 through the optical pickup to which the reflected light carries out photo electric translation. This is answered, and the BCA regenerative circuit 1720 generates the disk ID signal 1715 based on the regenerative signal inputted, and outputs it to the 2nd code decoder 1722.

[0190] Furthermore, the laser beam outputted from an optical pickup irradiates the key information record section 1605 of an optical disk 1601, and is inputted into the key information playback section 1723 through the optical pickup to which the reflected light carries out photo electric translation. This is answered, and the key information playback section 1723 generates the data of a key (DK) based on the regenerative signal inputted, and outputs them to the 2nd code decoder 1722. The 2nd code decoder 1722 decodes the enciphered contents which are outputted from the data playback section 1721 using the inputted disk ID signal 1715, and a key (DK) and the decode key which consists of a title code 1716 of the above-mentioned contents. Decryption processing of the 2nd code decoder 1722 is expressed with a degree type. When contents are picture signals, an MPEG signal is elongated and a picture signal is outputted from the 2nd code decoder 1722.

[0191]

[Equation 15]

C[FK]#(DK*BCA*T)

= C[FK] #FK=C [0192] The above-mentioned encryption contents can always be reproduced, without carrying out access with key issuance pin center,large equipment 1707 by recording the data of a key (DK) on the key information record section 1605 once. Moreover, since all decode keys required for decryption processing are recorded on the optical disk 1601, the above-mentioned optical disk 1601 is reproducible with the optical disk record regenerative apparatus of the arbitration which has the BCA regenerative circuit 1720, the key information playback section 1723, and the 2nd code

decoder 1722.

[0193] Furthermore, since a disk ID signal which is different in the above-mentioned optical disk 1601 from the BCA regenerative circuit 1720 is outputted when the above-mentioned encryption contents tend to be copied to the optical disk 1601 with which Disks ID differ and it is going to reproduce, the enciphered contents cannot be decoded, and contents are not reproduced even if copied. However, a decode key may be received after accounting also in this case by transmitting the title and Disk ID of contents to a key issuance pin center,large by the network or oral. Thus, even if the enciphered contents are copied by another optical disk 1601, since accounting surely follows in case the optical disk 1601 which copied the contents which are not reproduced unjustly and enciphered is played, copyright can be protected.

[0194] Drawing 23 is the table showing the configuration of ID grant table concerning the 5th operation gestalt, and arranges and shows the key (K) inputted into the 1st code decoder 1713 in case a system ID differs from Disk ID, and the key (DK) inputted into the key information record circuit 1719. In drawing 23 , T1, T2, and T3 are the title codes of different contents, and FK1, FK2, and FK3 are the decode keys for decoding the encryption contents which have T1, T2, and the title code of T3, respectively. Moreover, DID1, DID2, and DID3 are the system IDs of a different CATV decoder 1706, respectively, and BCAS1, BCAS2, and BCAS3 are the disks ID of a different optical disk 1601, respectively. At this time, the key (Kmn) inputted into the CATV decoder 1706 is determined that it will satisfy a degree type.

[0195]

[Equation 16] FKn=Kmn*Tn*DID*TIMEn [0196] Moreover, the key (DKmn) inputted into the optical disk record regenerative apparatus 1714 is determined that it will satisfy a degree type.

[0197]

[Equation 17] FKn=DKmn*BCAm*Tn [0198] As shown in drawing 23 , when contents differ, even when contents are the same, of course, protection of the copyright ranging from a different CATV decoder 1706 and a different optical disk differing from different key information which comes to hand from key issuance pin center,large equipment 1707 for every broadcasting hours to details is attained. Similarly, if a system ID and Disk ID differ from a hour entry but, since [with the same contents] key information differs, CATV firm equipment 1701 does not need to change encryption contents for every user, and should just prepare one encryption contents to one contents. The system at the time of broadcast can be simplified by this, and offer of the contents to the viewer of a large quantity is attained by low cost.

[0199] In addition, although this operation gestalt explained the case where the contents from the head end of cable television were broadcast, the same is said of broadcast by the electric wave.

[0200] The optical disk concerning a <effectiveness of 3rd thru/or 5th operation gestalt> book operation gestalt has the user data area which can record informational the 1st information field where the 1st disk information is recorded, the 2nd information field where the 2nd disk information for identifying each disk is recorded, and by irradiating a light beam. Therefore, management of an optical disk is easily realizable by adding the information which identifies the above-mentioned optical disk to the optical disk of the conventional technique. Here, preferably, the information field of the above 2nd is recorded in the information field of the above 1st, and can be reproduced by the optical pickup which reproduces the information field of the above 1st. Moreover, the information field of the above 2nd is recorded by removing selectively the record film in the information field of the above 1st so that it may be a long configuration and two or more trimming fields may be formed radially, and can prevent that the 2nd disk information of the above is altered easily.

[0201] Moreover, the 1st information field where the 1st disk information is recorded according to the record approach of the encryption contents concerning this operation gestalt, The 2nd information field where the 2nd disk information for identifying each disk is recorded, In case the data of contents are recorded on the above-mentioned user data area of the optical disk which has the user data area which can record informational by irradiating a light beam The data of contents are enciphered and recorded so that the data of contents may be decoded by the operation using the 2nd disk information of the above at least and it can reproduce. Therefore, using the identification information of the optical disk which exists only in the specific optical disk of one sheet, by enciphering contents, the unjust copy of contents can be prevented and there is characteristic effectiveness that copyright can be protected.

[0202] Furthermore, the optical disk concerning this operation gestalt has the key information record section which records the key information for decoding the contents which were enciphered and were recorded in the user data area. Therefore, there is characteristic effectiveness of it becoming unnecessary to input key information, whenever it reproduces by recording key information on a key information record section once in the system which needs key information, in case the contents enciphered and recorded are decoded.

[0203] Furthermore, according to the record approach of the encryption contents concerning this operation gestalt The 1st information field where the 1st disk

information is recorded, and the 2nd information field where the 2nd disk information for identifying each disk is recorded, By irradiating a light beam, the user data area which can record informational, In case contents are recorded on the above-mentioned user data area of the optical disk which has the key information record section which records the key information for decoding the data of the contents which were enciphered and were recorded in the user data area The data of contents are enciphered and recorded as the data of contents can be decoded at least by the operation using the 2nd disk information of the above, and the above-mentioned key information and it can reproduce. Therefore, even if the data of the enciphered contents are copied by another optical disk, since accounting surely follows in case the optical disk which copied the data of the contents which are not reproduced unjustly and enciphered is played, copyright can be protected.

[0204] Here, the 1st disk information is preferably constituted by the very small concavo-convex pit, and the 2nd disk information for identifying an optical disk is recorded on the above-mentioned concavo-convex pit. Therefore, it can prevent that the 2nd disk information is altered easily. Furthermore, preferably, it is formed so that the 1st disk information of the above and the 2nd disk information may adjoin. Since the 1st disk information can be continued and it can reproduce in case the 2nd disk information can also be continuously reproduced by this in case the 1st disk information of the above is reproduced, or the 2nd disk information is reproduced, it becomes possible to bring forward the processing for the 2nd disk information for CPU identifying a disk promptly coming to hand, in case an optical disk is started, for example, and recording the enciphered contents.

[0205] Moreover , the system at the time of broadcast can be simplify by this that what is necessary be for CATV firm equipment 701 if a system ID and Disk ID differ from a hour entry but , since [with the same contents] key information differ not to change encryption contents for every user according to the record approach of the encryption data concerning this operation gestalt , and just to prepare one encryption contents to one contents , it be a low cost , and offer of the contents to the viewer of a large quantity be attain .

[0206] In the 3rd [beyond <the modification of the 3rd and 5th operation gestalten>], and 5th operation gestalt Although the trimming fields 1105 and 1606 are formed in BCA 1104 and 1604 located in the control user data area 1102 and the inner circumference section in 1602, respectively as shown in drawing 16 and drawing 21 As this invention is shown in drawing 24 and drawing 25 which show the data storage area of not only this but the optical disks 1101a and 1601a applied to the modification of the

3rd and 5th operation gestalt, respectively Record film may be trimmed and the trimming fields 1105a and 1606a may be formed so that the control user data areas 1102 and 1602 may be overflowed into the inner circumference side of an optical disk. That is, BCA(s) 1104a and 1604a are not contained in the control user data area 1102 and 1602, but from the inner circumference section of the control user data areas 1102 and 1602, it is arranged and they are formed, respectively so that it may overflow inside the control user data areas 1102 and 1602. In this modification, BCA(s) 1104a and 1604a are formed in this way, because the margin in case the path of the spot of the beam of a laser beam changes with the instability of a focus servo circuit is taken into consideration. Also in this modification, in order to protect so that the data recorded on these user data areas 1103 and 1602 may not be destroyed since the user data areas 1103 and 1603 exist in the outside of the controller user data areas 1102 and 1602, the trimming fields 1105a and 1606a are arranged and formed.

[0207] <Operation gestalt of ** 6th> drawing 26 is the block diagram showing the configuration of the user data area in the optical disk which is the 6th operation gestalt concerning this invention, and the configuration of the optical disk regenerative apparatus which decodes encryption contents from the data of a user data area. In this operation gestalt, optical disks are record mold optical disks, such as DVD-RAM.

[0208] As shown in drawing 26 , the user data area 2150 consists of a sector header field 2101, a Maine data area 2102, and error detecting code 2103. While the copyright control information 2105 by which the copyright control information (a scramble flag, copy control information, etc. are included.) about the sector address 2104 which shows the location of a sector, and the data recorded on the Maine data area 2102 is recorded on the sector header field 2101 is recorded, the sector head field 2101 includes the decode key field 2106 for decoding, when the code is given to the data of the Maine data area 2102. Moreover, the Maine data area 2102 is divided into the field where the non-enciphering contents 2107 are recorded, and the field to which the encryption contents 2108 are recorded, and the non-enciphering contents 2107 include the alignment pattern in MPEG, and control information of the data which follow, such as various control information. Furthermore, the encryption contents 2108 contain the data of contents with which AV data which mainly need protection of copyrights were enciphered.

[0209] The decode key for reproducing the Maine data area 2102 which follows is divided and recorded on the decode key (henceforth a division decode key) with which the plurality which has predetermined size was divided by the decode key field 2106. For example, to 4 bytes of one decode key field, when a decode key is 8 bytes, 8 bytes of

decode key is divided into 4 bytes each of division decode key, and two divided division decode keys are recorded on the decode key fields 2106 and 2109 of two sectors which continue logically, respectively. At the time of playback of such a user data area, two or more division decode keys divided from the decode key fields 2106 and 2109 of two or more (however, an unusable sector is skipped according to a defect etc.) sectors which continue logically are acquired, the division decode key of the acquired required number is connected with the data coupler 2111, and an encryption decode key (8 bytes) required for playback is obtained at it. According to the content of each copyright control information 2105, decryption processing is performed using a decoder 2114 to the data recorded on the Maine data area 2102 of the sector which was able to obtain the encryption decode key (8 bytes).

[0210] Furthermore, it is also possible to encipher to a decode key, in order to raise the reinforcement of a code more, and even if it is the same cryptographic key by adding the decode key translation data which is the information in data to a key so that the result of a code may not become fixed, it is also possible to offer a different code result. As shown in drawing 26 , the encryption decode key outputted from the data coupler 2111 is inputted into the key decoder 2112, and the key decoder 2112 decrypts the inputted encryption decode key using a predetermined disk key in the padding data (1 byte) and the decode key (7 bytes) which are dummy data, and, specifically, outputs it to the key converter 2113. Here, a disk key is acquired by decoding the encryption disk key recorded on the optical disk with a disk key decoder (not shown) using the private key which is a predetermined master key. Subsequently, by carrying out data conversion of the decode key translation data 2110 read from the Maine data area 2102 by predetermined conversion operations, such as multiplication, and a division, an operation using a predetermined weighting factor, using the decode key outputted from the above-mentioned key decoder 2112, the key transducer 2113 generates a contents decode key (7 bytes), and outputs it to a decoder 2114. And a decoder 2114 generates and outputs the data of the decrypted contents by decoding the data of the contents read from the Maine data area 2102 using the contents decode key (7 bytes) outputted from the above-mentioned key transducer 2113. In addition, it is desirable to use the data which unjust utilization of data can detect immediately as decode key translation data 2110 by carrying out the alteration of copy generation-control information, the macro vision control flag of an analog, etc.

[0211] Drawing 27 is the block diagram showing the copyright control information to a user data area, arrangement of a decode key, and arrangement of the encryption contents to the Maine data area in the optical disk concerning the 6th operation gestalt.

In an example of the user data area 2150 illustrated by drawing 27 , the decode key field is divided and arranged to the 1st decode key field 2201 which has 4 bytes of division decode key, and the 2nd decode key field 2202 which has 4 bytes of division decode key. For this reason, it will not be based on the magnitude of encryption contents recorded on these two sectors, but two or more sectors (drawing 27 two sectors) will be used. In this case, dummy data is recorded on an intact field as complement data. In the example of drawing 27 , when there are only the encryption contents 2204 for 1 sector, the complement data 2203 for 1 sector are recorded.

[0212] Drawing 28 is the block diagram showing arrangement in case the unit of an error correction straddles two or more sectors in the optical disk concerning the 6th operation gestalt. For example, when an optical disk is DVD, the capacity of an error correction is heightened by using the unit block (henceforth an ECC block) of the error correction code of 16 sector. For this reason, in case record and playback of data are performed, record in an ECC block unit is needed. Supposing it records by dividing a decode key into two or more division decode keys of arbitration, the case where one decode key is recorded ranging over two or more error correction blocks will occur. In the case of playback, since it is necessary to reproduce two or more divided division decode keys of all, it is necessary to reproduce to an ECC block just before recording the decode key besides the sector which recorded the data of encryption contents. In the example of drawing 28 , it is characterized by setting the number of partitions when dividing a decode key as the divisor of the number of sectors of an ECC block. It is lost that two or more divided division decode keys are recorded by this ranging over an ECC block. Furthermore, when AV data to record do not fulfill an ECC block, using only one kind of decode key as a decode key used within one ECC block, it can prevent reading the data of an unnecessary sector from an optical disk at the time of playback by arranging a complement sector in complement data and a list.

[0213] <Operation gestalt of ** 7th> drawing 29 is the block diagram showing the configuration of the lead-in groove field 2401 in the optical disk which is the 7th operation gestalt concerning this invention, and the user data area 2402, and the configuration of the optical disk regenerative apparatus which decodes encryption contents from the data of the lead-in groove field 2401 and the user data area 2402.

[0214] In drawing 29 , the lead-in groove field 2401 and the user data area 2402 consist of sectors which have the sector header field 2101, the Maine data area 2102, and error detecting code 2103 like the 6th operation gestalt of drawing 26 , respectively. The sector address 2104 which shows the location of a sector to the sector header field 2101, Copyright control information about the data recorded on the Maine data area 2102 (a

scramble flag, copy control information, etc. are included.) While the copyright control information 2105 recorded is recorded, the sector header field 2101 The record location of a decode key for referring to the decode key for decoding, when the code is given to the data of the Maine data area 2102 (the record location or storing location in the decode key table 2404 in the Maine data area 2102 is said.) The key index area 2403 which records the shown key index is included. The decode key for decoding the encryption contents recorded on the user data area 2402 is recorded on the lead-in groove field 2401 rewritable in a table format in the form of the decode key table 2404. The decode key recorded on the lead-in groove field 2401 by the key index recorded on the key index area 2403 is referred to. After the decode key by which reference was carried out [above-mentioned] is decoded by padding data and the decode key (or title key) like the 6th operation gestalt illustrated by drawing 26 with the key decoder 2112 which uses a predetermined disk key, the decode key (or title key) by which decode was carried out [above-mentioned] is changed into a contents decode key by the key converter 2113 which uses decode key translation data, and is outputted to a decoder 2114. A decoder 2114 generates and outputs the data of decryption contents by decoding the data of the enciphered contents using a contents decode key.

[0215] In the optical disk and optical disk regenerative apparatus concerning the 7th operation gestalt constituted as mentioned above, the size of the key index area 2403 can assign the decode key size of the decode key table 2404 independently by recording the key index for reference on the key index area 2403 in the sector header field 2101. Moreover, even after assigning the size of the decode key table 2404, the decode key of free size can be used by using two or more decode keys continuously from the decode key table 2404 shown by the key index in the key index area 2403.

[0216] Drawing 30 (a) is the block diagram showing the data configuration in the case of displaying the condition of not recording, with the initial value of a decode key in the Maine data area 2102 of the lead-in groove field 2401 in the optical disk concerning the 7th operation gestalt. In drawing 30 (a), the condition [of not recording] data 2501 which are the known fixed value (for example, data, such as oar 0) which is not used as a key as initial value of the decode key recorded in the time of a format of an optical disk etc. are recorded, and this shows the condition of a decode key of not recording.

[0217] Drawing 30 (b) is the block diagram showing the data configuration in the case of displaying a record condition on a decode key condition table in the Maine data area 2102 of the lead-in groove field 2401 in the optical disk concerning the 7th operation gestalt. In drawing 30 (b), like the decode key illustrated by drawing 30 (a), the decode key condition table 2502 of the table format which can be referred to with an index has

been arranged to the lead-in groove field 2401, and the record condition of a decode key is indicated as follows as record condition data 2503.
(1) 0x00:intactness, (2)0x01:field reservation, (3)0x03:key record ending and (4), others : reserved.
Here, 0x show a hexadecimal display about the alphabetic character following it.
[0218] Drawing 31 is the block diagram showing arrangement of a decode key in the optical disk concerning the 7th operation gestalt. In the example of drawing 31 , in order to raise the dependability of a decode key, arrangement of the decode key field to a disk top is devised. Usually, since defective management is performed in the user data area 2602, when a write-in defect occurs, shift processing is performed to an alternative field etc. However, the above defective managements are not performed in the lead-in groove field 2601. for this reason, reading appearance is carried out and there are a write-in defect and a case where it becomes impossible using a decode key required for playback of AV data, and it becomes still more impossible the optical disk's itself using it according to a defect's etc. generating. Therefore, it is desirable to cover two or more different ECC blocks, and to record the decode key of sum total plurality. Moreover, when two or more decode keys are recorded on the field which approached, there is a case where it becomes impossible to read all the things recorded with a blemish, dust, etc. [two or more] For this reason, as shown in drawing 31 , in the lead-in groove field 2601 and the lead-out field 2603, it is more desirable respectively to record each decode key on the location distant on the layout like the inner circumference side of an optical disk and a periphery side.
[0219] In addition, in the operation gestalt of drawing 29 , the decode key field is arranged to the lead-in groove fields 2401 and 2601. This is for raising safety in case the user data area 2602 accesses from the drive equipment of a personal computer etc. in consideration of being an accessible field by a usual lead command and a usual light command. Therefore, the same effectiveness can be acquired even if it arranges these to the user data area 2602.
[0220] <Operation gestalt of ** 8th> drawing 32 is the block diagram showing the data configuration when managing the data of the optical disk which is the 8th operation gestalt concerning this invention with file management system. In the example of drawing 32 , the sector address in which the desired file was stored is managed based on the structure of a file system.
[0221] With the structure of the file system specified by International Organization for Standardization in ISO13346, since it corresponds to a rewritable mold optical disk, the record location of a file is managed using the information called a file entry. As shown in

drawing 32 , the data of the record location of file (1) 2703 are stored as file entry (1) 2701 in the file management information field 2751, and the data of the record location of file (2) 2704 are stored as file entry (2) 2702. Each file consists of extents 2705 and 2706 which manage the field of two or more sectors which continued on the optical disk. On an optical disk, the encryption contents shown with the 7th operation gestalt are recorded in the Maine data area 2102 which a file entry shows, and a decode key is recorded on the decode key table 2707 in the lead-in groove field 2601. The pointer in which the record location for referring to a decode key required for decode is shown is recorded on the sector header field 2101 in the user data area 2602 where encryption contents were recorded in the key index area 2708. In addition, although the decode key is managed and recorded per a file unit and extent with this operation gestalt, this invention may manage and record a decode key at least by one of not only this but a file unit, and the extent units.

[0222] In the optical disk managed by the file system as mentioned above, the record actuation of contents which needs protection of copyrights is explained using drawing 33 . Drawing 33 shows the record processing of contents which is performed by the file management system concerning the 8th operation gestalt and which needs protection of copyrights.

[0223] In the case of record of encryption contents, the decode key condition table 2502 illustrated by drawing 30 (b) is first read in step S2801, and the free area of the decode key table 2707 is investigated at it. Subsequently, in step S2802, since it is judged whether there is any free area of the decode key table 2707, and the decode key to encryption contents cannot be recorded when it is NO, record actuation is stopped in step S2807, and record processing of the contents concerned is ended. On the other hand, when it is YES at step S2802, and a decode key [finishing / acquisition] (or title key) is recorded and the decode key cannot be acquired, a decode key field is reserved. Subsequently, at step S2804, after setting up the key index recorded on the copyright control information (the information on whether it enciphers or not, the information on classification which shows the class of encryption are included.) and the key index area 2708 of the contents to record, contents are enciphered in step S2805 and it records on an optical disk by file format per extent. At this time, the same copyright control information and a key index may be used per file, and these may be changed per extent. that is, on the other hand in steps S2804 and S2805, it comes out of the unit to process of a file unit and the extent units at least. After updating file management information for managing the data by which record was carried out [above-mentioned] in step S2806 finally based on the information about the recorded contents, record processing of

the contents concerned is ended.

[0224] Drawing 34 is a flow chart which is performed by the file management system concerning the 8th operation gestalt and which shows regeneration of contents. Drawing 34 shows the processing which reproduces the contents recorded by file format by the approach shown in drawing 33 from an optical disk.

[0225] In case playback actuation of a file is performed, in order to know the field of the decode key table which the file to reproduce is using, the key index to the field shown by the file entry in the file management information field 2751 is acquired. after acquiring by carrying out reading appearance of the file entry of the file reproduced from the file management information 2751 in step S2901, and reproducing, specifically, it acquires by carrying out reading appearance of the value of a key index area, and reproducing in step S2902, from the sector header field 2102 of the field shown by the file entry. When a different code per extent is being performed, in each extent, the key index area in a sector header is read. Subsequently, in step S2903, it acquires by reading a decode key from the decode key field of the decode key table 2707 shown by the acquired key index, and reproducing. Furthermore, in step S2904, the data of the contents in a file are read from the field shown by the file entry, it reproduces, and the data of the reproduced contents are decoded. Here, if playback and decode of contents of a file are completed, regeneration of the contents concerned will be ended.

[0226] Drawing 35 is a flow chart which is performed by the file management system concerning the 8th operation gestalt and which shows the deletion of contents, and shows the actuation which deletes the data of the contents of file format recorded by the approach shown in drawing 33 by drawing 35 .

[0227] In case deletion actuation of a file is performed, in order to know the field of the decode key table 2707 which the file to delete is using, the key index to the field shown by the file entry is acquired. After specifically acquiring the file entry of the file deleted from the file management information in the file management information field 2751 in step S3001, the value of a key index area is acquired from the sector header of the field shown by the file entry in step S3002. Here, when a different code per extent is being performed, in each extent, the key index area in a sector header is read. Subsequently, after opening a decode key from the decode key field of the decode key table 2707 shown by the acquired key index (here, it says that disconnection of a decode key deletes the decode key concerned from the table concerned.), the file entry which shows the write-in location of the file deleted in step S3004 deletes from file-management information, and the deletion of the contents concerned ends in step S3003. In the conventional file system, when deleting a file, only the file entry was deleted, but since the record sector

of a decode key and encryption contents is recorded on another field, the decode key recorded on another field cannot be deleted. In the above-mentioned operation gestalt, the decode key on an optical disk is managed by deleting the decode key which the key index in a sector header field shows from the decode key table 2707 in advance of deletion of a file entry.

[0228] <Operation gestalt of ** 9th> drawing 36 is the block diagram showing the configuration of the optical disc system which is the 9th operation gestalt concerning this invention, and this optical disc system is information processing system which records and reproduces the contents which need protection of copyrights for an optical disk 3100. The optical disc system concerned is equipped with encoding equipment 3101, an optical disk unit 3102, decoding equipment 3103, and a personal computer 3104, and is constituted.

[0229] The contents memory 3131 in which encoding equipment 3101 stores the data of contents, The coding network 3132 encoded in the form of an MPEG format of the data of the above-mentioned contents, The cryptographic key memory 3133 which stores a cryptographic key, and the code circuit 3134 which generates a decode key and is stored in the decode key memory 3111 while enciphering the data of the encoded contents using a cryptographic key, The decode key memory 3111 which stores a decode key, and the bus code circuit 3112 which carries out bus encryption of the decode key, It has the interface 3124 which transmits data and the decode key of the contents which were connected to the interface 3122 of a personal computer 3104 through PCI bus 3151, and were enciphered. Moreover, the decode key table memory 3113 in which an optical disk unit 3102 stores two or more decode keys, A bus code and a decoder circuit 3114, and the record regenerative circuit 3119 that reads data from an optical disk 3100 and is reproduced while recording data to an optical disk 3100, It has the interface 3120 which is connected with the interface 3121 of a personal computer 3104 through the SCSI bus 3152, and performs processing of signal transformation, protocol conversion, etc. in transmission and the receiving list of data or a signal. In addition, the SCSI bus 3152 may be an ATAPI bus. Here, the encryption processing which uses bus encryption and a bus decryption in order to encipher a cryptographic key and a decode key, to transmit and to receive on PCI bus 3151 or the SCSI bus 3152, respectively, and decryption processing are said.

[0230] Furthermore, the personal computer 3104 The control section 3130 which controls the actuation, and the bus encryption decode key table memory 3115 which stores two or more bus encryption decode keys, Two or more decode key statuses corresponding to two or more above-mentioned bus encryption decode keys (the record

condition of a decode key is shown and, specifically, finishing [intactness, field reservation, key record ending, and reservation] etc. is shown.) It connects with the interface 3120 of the decode key condition table memory 3116 which stores data, and an optical disk unit 3102 through the SCSI bus 3152. In transmission and the receiving list of data or a signal Signal transformation, The interface 3121 which performs processing of protocol conversion etc., It connects with the interface 3123 of decoding equipment 3103, and the interface 3124 of encoding equipment 3101 through PCI bus 3151. In transmission and the receiving list of data or a signal Signal transformation, It has the interface 3122 which performs processing of protocol conversion etc. Decoding equipment 3103 is connected with the interface 3122 of a personal computer 3104. In transmission and the receiving list of data or a signal Furthermore, signal transformation, The interface 3123 which performs processing of protocol conversion etc., The bus decoder circuit 3117 which carries out the bus decryption of the encryption decode key received with an interface 3123, While decoding the data of the decode key memory 3118 which stores a decode key, and the encryption contents received with an interface 3123 using the decode key of the decode key memory 3118 It has the decryption circuit 3141 which performs decryption processing of an MPEG format, generates a picture signal and a sound signal, and is outputted to a display unit 3105.

[0231] In the encoding equipment 3101 of this optical disc system A coding network 3132 is encoded in the form of a format of the data of contents, such as AV data stored or inputted into the contents memory 3131, of MPEG. The code circuit 3134 enciphers the data of the contents by which coding was carried out [above-mentioned] using the cryptographic key in the cryptographic key memory 3133 generated in order to avoid unjust utilization of the contents on a personal computer 3104. The data of the enciphered contents are transmitted to an optical disk unit 3102 through an interface 3124 and a personal computer 3104. Here, the data of the enciphered contents are transmitted to the record regenerative circuit 3119 through PCI bus 3151, the interface 3122 of a personal computer 3104 and an interface 3121, and the interface 3120 of an optical disk unit 3102 from the interface 3124 of encoding equipment 3101. And the data of the enciphered contents are recorded on an optical disk 3100 by the record regenerative circuit 3119 of an optical disk unit 3102. Moreover, the record regenerative circuit 3119 of an optical disk unit 3102 reproduces the data of the encryption contents currently recorded on the optical disk 3100, and transmits the data of the reproduced encryption contents to the decryption circuit 3141 through an interface 3120, the interface 3121 of a personal computer 3104 and an interface 3122, and the interface 3123 of decoding equipment 3103. The decryption circuit 3141 of decoding equipment

3103 decrypts the code to the data of encryption contents, and performs decryption processing of an MPEG format, and outputs the picture signal and sound signal of contents which were decrypted to a display unit 3105 or loudspeaker equipment (not shown), respectively.

[0232] The code circuit 3134 of encoding equipment 3101 generates a decode key required at the time of playback, and stores it in the decode key memory 3111 at the same time it enciphers to the data of the contents encoded in the form of the MPEG format using the cryptographic key in the cryptographic key memory 3133. Although it is necessary to record the data and the decode key of contents which were encoded on an optical disk 3100, when dealing with a decode key on a personal computer 3104 with a plaintext, decode of the data of the enciphered contents may become easy by reading a decode key from an optical disk 3100. In order to avoid this, while performing mutual recognition, a bus code is performed between encoding equipment 3101 and an optical disk unit 3102 using the bus key shared mutually.

[0233] That is, after, as for the decode key in the decode key memory 3111, encryption is given by the bus code circuit 3112 of encoding equipment 3101, specifically, the encryption decode key is stored in the bus encryption decode key table memory 3115 of a personal computer 3104 through an interface 3124, PCI bus 3151, and an interface 3122. On the other hand, after a decryption of the encryption decode key reproduced by the record regenerative circuit 3119 from the optical disk 3100 is performed in the bus code and decoder circuit 3114 of an optical disk unit 3102, the decrypted decode key is stored in the decode key table memory 3113. Moreover, a bus code and a decoder circuit 3114 are recorded on an optical disk 3100 through the record regenerative circuit 3119, after receiving and carrying out a bus decryption through an interface 3121, the SCSI bus 3152, and an interface 3120 from the bus encryption decode key table memory 3115 and storing the updated decode key by which bus encryption was carried out in the decode key table memory 3113.

[0234] Moreover, a decode key condition table is transmitted and stored in the decode key condition table memory 3116 through an interface 3120, the SCSI bus 3152, and an interface 3121, after the record regenerative circuit 3119 is reproduced from an optical disk 3100. Furthermore, after reading appearance of the decode key condition table updated with the personal computer 3104 is carried out from the decode key condition table memory 3116 and being transmitted to the record regenerative circuit 3119 through an interface 3121, the SCSI bus 3152, and an interface 3120, the record regenerative circuit 3119 records the received decode key condition table on an optical disk 3100. Therefore, on the personal computer 3104 located in the medium, only the

enciphered decode key will be dealt with using the bus encryption decode key table 3115 and the decode key condition table memory 3116 which store two or more bus encryption decode keys, and much more safety will be secured.

[0235] Much more safety is secured by performing the bus code of a decode key similarly between an optical disk unit 3102 and decoding equipment 3103. Namely, the bus decoder circuit 3117 of decoding equipment 3103 decodes the encryption decode key received through the interface 3123 from the personal computer 3104, and stores it in the decode key memory 3118. The decryption circuit 3141 decodes the data of the contents enciphered using the decode key in the decode key memory 3118.

[0236] As shown in the 7th above-mentioned operation gestalt, in recording the decode key for decoding the data of the contents enciphered on the optical disk 3100 in a table format, after carrying out the bus encryption of the decode key table reproduced on the optical disk unit 3102 by the bus code and the decoder circuit 3114, the data of the decode key table by which bus encryption was carried out transmit and store in the bus encryption decode key table memory 3115 of a personal computer 3104 through an interface 3120. When recording the data of contents, a personal computer 3104 investigates by searching with a plaintext the free area of a decode key condition table to the decode key table currently recorded on the optical disk 3100, and assigns the decode key which is transmitted from encoding equipment 3101 and by which bus encryption was carried out to a free area. If a code (for example, block cipher in a decode key long unit) which is completed per decode key as a bus code is used at this time, a decode key does not have to decode and it is not necessary to carry out a re-code at the time of assignment to a decode key block.

[0237] In addition, since an optical disk unit 3100, an optical disk unit 3102, and the decode key table and decode key condition table transmitted and stored a personal computer 3104 and in between are data of a block of one lump, respectively, it can be called block data.

[0238] Only a decode key required for a decryption of the contents which it is going to reproduce from the decode key block reproduced from the optical disk unit 3102 is searched and extracted from the bus encryption decode key table memory 3115, through the bus decoder circuit 3117 of a personal computer 3104 and decoding equipment 3103, it transmits to the decode key memory 3118, and the case at the time of playback of contents is also stored in it. And the decryption circuit 3141 receives enciphered AV data which were reproduced by the record regenerative circuit 3119 of an optical disk unit 3102 from the optical disk 3100 through a personal computer 3104 and an interface 3123, and decrypts and outputs received AV data which were enciphered to a picture

signal or a sound signal using the decode key in the decode key memory 3118. If a code (for example, block cipher in a decode key long unit) which is completed per decode key as a bus code like the time of record of above-mentioned contents is used also in this case, when sampling the decode key from a decode key block, a decode key does not have to decode and it is not necessary to carry out a re-code. Furthermore, it can carry out to that the escape of a decode key field, such as assigning two or more decode keys, is easy on a personal computer 3104, and insurance, without changing the configuration of an optical disk unit 3102, in enlarging size of a decode key.

[0239] <Operation gestalt of ** 10th> drawing 37 is the block diagram showing the configuration of the user data area in the optical disk which is the 10th operation gestalt concerning this invention, the configuration of the optical disk recording apparatus which carries out the code of the contents and is recorded on a user data area, and the configuration of the optical disk regenerative apparatus which decodes encryption contents from the data of a user data area. This 10th operation gestalt is characterized by adding the configuration of an optical disk recording device in the 6th operation gestalt, and explains it to a detail about this configuration.

[0240] In an optical disk recording device, in order to raise the reinforcement of a code so that the result of a code may not become fixed, after calculating key conversion predetermined [, such as an operation using multiplication, a division, and a predetermined weighting factor,] by the key converter 2119 using the decode key translation data which is the information in contents about the cryptographic key inputted and obtaining a contents decode key, the data of contents are enciphered using the contents decode key concerned.

[0241] That is, the cryptographic key for enciphering the data of contents and the data of contents at the time of record of contents is inputted into an optical disk recording device. Here, the data of contents are inputted into the key converter 2119 and the code machine 2120, and a cryptographic key is inputted into the key code machine 2118 and the key converter 2119. To the cryptographic key by which the input was carried out [above-mentioned], by calculating predetermined key conversion using the 1st and 2nd decode key translation data 2115 and 2116 which is a part of information in contents, the key converter 2119 generates a contents decode key, and outputs it to the code machine 2120. Subsequently, the code machine 2120 enciphers the data of the above-mentioned contents by which an input is carried out using the above-mentioned contents decode key, and records encryption contents on AV data-logging sector 2152 in the user data area 2150 of an optical disk.

[0242] Here, the 1st decode key translation data 2115 which is the copy control

information containing the 2nd decode key translation data 2116 which is the information in AV data which differ in general per sector as decode key translation data used in an optical disk regenerative apparatus, the copy generation-control information included in the sector on which control information was recorded, the macro vision control flag of an analog, etc. is used. By using the 2nd former decode key translation data, it becomes possible to restore the contents decode key for enciphering the data of contents by the key converter 2113 according to the content of the 2nd decode key translation data the whole sector. Moreover, since the 1st latter decode key translation data is data which can detect unjust utilization of data easily at the time of the alteration, when the 1st decode key translation data concerned is altered, the effectiveness that it can perform easily carrying out by the ability not decoding the data of contents is acquired. A cryptographic key is changed into a decode key by the predetermined conversion operation, using the data which are the playback control record sector on which the playback control information used for playback control of AV data is specifically recorded as 1st decode key translation data, and this is used as a contents decode key in the code machine 2120. Furthermore, the 1st decode key translation data which is data of a playback control record sector, A cryptographic key by carrying out a predetermined conversion operation using two decode key translation data containing the 2nd decode key translation data which is some non-enciphering contents where the enciphered contents are recorded, and which are sectors Another contents decode key may be calculated and this another contents decode key may be used as a contents decode key in the code machine 2120.

[0243] On the other hand, the key code machine 2118 generates an encryption decode key by enciphering using the disk key into which the above-mentioned cryptographic key by which an input is carried out is inputted like an optical disk regenerative apparatus. Since the decode key fields 2106 and 2109 in a sector header field are small, after the data divider 2121 divides an encryption decode key into two or more division decode keys as compared with the size of this encryption decode key, each division decode key is recorded on different decode key fields 2106 and 2109. In the example of drawing 37 , an encryption decode key is divided into two encryption division decode keys, and is recorded on the decode key fields 2106 and 2109 of two sectors which continue, respectively. Here, since it has enciphered to the decode key which is a cryptographic key with the key code vessel 2118, the reinforcement of the code to a cryptographic key can be raised.

[0244] Using the information on the 1st above-mentioned decode key translation data 2115 and the 2nd decode key translation data 2116, by calculating predetermined key

conversion of the decode key from the key decoder 2112, the key transducer 2113 generates a contents decode key, and outputs it to a decoder 2114 at the time of playback of contents. Subsequently, a decoder 2114 obtains decryption contents by decoding the data of encryption contents using this contents decode key. Here, the key transducer 2113 may calculate predetermined key conversion of the decode key from the key decoder 2112 using the information only on the 1st decode key translation data 2115.

[0245] <Operation gestalt of ** 11th> drawing 38 is the block diagram showing the configuration of the user data area in the optical disk which is the 11th operation gestalt concerning this invention, the configuration of the optical disk recording apparatus which carries out the code of the contents and is recorded on a user data area, and the configuration of the optical disk regenerative apparatus which decodes encryption contents from the data of a user data area. This 11th operation gestalt is characterized by adding the configuration of an optical disk recording device in the 7th operation gestalt, and explains it to a detail about this configuration.

[0246] The key code machine 2118 which enciphers a cryptographic key like the 10th operation gestalt of drawing 37 in drawing 38 using a predetermined disk key as for an optical disk recording apparatus, It has the key converter 2119 which calculates predetermined key conversion to a cryptographic key using the 1st [in contents], and 2nd decode key translation data 2115 and 2116, and calculates a contents decode key, and the code machine 2120 which enciphers contents using the above-mentioned contents decode key, and is constituted. Here, the decode key outputted from the key code machine 2118 is recorded on the Maine data area 2102 in the lead-in groove field 2401. On the other hand, an optical disk regenerative apparatus is equipped with the key decoder 2112, the key converter 2113, and a decoder 2114 like the 7th operation gestalt of drawing 29 , and is constituted. Here, reading appearance of the decode key recorded on the Maine data area 2102 in the lead-in groove field 2401 is carried out, it is inputted into the key decoder 2112, and the key decoder 2112 decodes a decode key using a predetermined disk key, and outputs it to the key converter 2113. Moreover, using the 1st and 2nd decode key translation data 2115 and 2116, the key transducer 2113 calculates predetermined key conversion to the decode key from the key decoder 2112, calculates a contents decode key, and outputs it to a decoder 2114.

[0247] As explained in full detail beyond <the effectiveness of the 6th thru/or 9th operation gestalt>, the record mold optical disk concerning this operation gestalt By dividing and recording a decode key on the decode key field of the predetermined size arranged to the sector header field, or recording a variable-length decode key on the decode key field shown in the key index area arranged to the sector header field The

record mold optical disk which can use the decode key of free die length can be offered without being caught by the decode key field of the size beforehand specified to the sector header field. Thereby, according to the protection-of-copyrights level to the contents to record, the code using the key length of arbitration can be made available.

[0248] In the operation gestalt beyond <a desirable modification>, the above-mentioned disk identification information is constituted by PURIPITTO which cannot be rewritten, and has preferably a local identifier showing the area where a disk is used in the above-mentioned disk identification information. Moreover, in the above-mentioned disk identification information, it has preferably the data category identifier which shows the class of record and refreshable contents on an optical disk. Furthermore, preferably, it is enciphered using a private key and the above-mentioned disk identification information is recorded on a disk identification information field at the time of manufacture. Furthermore, the above-mentioned disk identification information contains the data showing the classification of desirable data recordable on a data-logging playback field, or the classification of data refreshable from a data-logging playback field.

[0249] In the above operation gestalt, it has the descrambling field managed table which manages preferably the response relation between the sector field where the data of contents are recorded, and a descrambling key. Moreover, the descrambling key area where a key management information field records preferably the descrambling key enciphered considering disk identification information as a key, The key information field which has a descrambling key status field showing the record condition of a descrambling key, The key-index field which recorded the pointer for referring to the contents information field which records the key information used at the time of the contents playback recorded on the disk, and a descrambling key required in order to reproduce contents is included. Furthermore, the pointer in which the field where a descrambling key is recorded with the data of the above-mentioned contents is shown preferably is recorded on the sector on which the data of contents are recorded.

[0250] In the above operation gestalt, the regenerative circuit of the disk identification information of an optical disk record regenerative apparatus is equipped with the circuit which decodes preferably the disk identification information enciphered using the private key. Moreover, in an optical disk record regenerative apparatus, the data enciphered considering disk identification information as a key are data of contents, such as image data and music data, preferably. Furthermore, preferably, disk identification information expresses the classification of data recordable on a data-logging playback field, and judges whether the regenerative circuit of disk

identification information is data of contents recordable [with the classification of the above-mentioned data]. Furthermore, the data decoded using disk identification information as a key are data of contents, such as image data and music data, preferably. Moreover, disk identification information expresses the classification of refreshable data from a data-logging playback field preferably, and the regenerative circuit of disk identification information judges whether it is data of refreshable contents by classification of the above-mentioned data.

[0251] In the above operation gestalt, the record circuit of contents records the descrambling key which solves the code given to the data of contents, such as enciphered image data and music data, and the data of the above-mentioned contents on the same sector preferably. Moreover, the regenerative circuit of contents reproduces the descrambling key which solves the code given to the data of contents, such as enciphered image data and music data, and the data of the above-mentioned contents from the same sector preferably.

[0252] In the above operation gestalt, the allocation circuit or approach of a key area arranges a field reserved flag to the descrambling key status field showing the record condition of a descrambling key preferably, records the information about the key used at the time of playback of the data of contents, and records the key index showing the record section of the descrambling key assigned to the data of contents. Moreover, preferably, the arrangement circuit or approach of a descrambling key reproduces the index of the descrambling key area used from contents from a contents information field, and arranges a recorded flag to the descrambling key status field shown in the key index corresponding to the descrambling key which arranges a descrambling key to the descrambling key area shown in the key index corresponding to the descrambling key to record, and is recorded on it.

[0253] In the above operation gestalt, preferably, an optical disk regenerative apparatus reproduces disk identification information, investigates whether contents are refreshable, reproduces key management information, reproduces the sector on which the data of contents, such as image data and music data, were recorded, and acquires a descrambling key from the reproduced sector. Furthermore, preferably, the data of the reproduced contents are descrambled by the descrambling key, and are outputted.

[0254] In the above operation gestalt, the approach of recording the data of contents The 1st information field where the 1st disk information is recorded preferably, The 2nd information field where the 2nd disk information for identifying each disk is recorded, In case contents are recorded on the above-mentioned user data area of the optical disk which has the user data area which can record informational by irradiating a light

beam, it enciphers and records so that it may decode by the operation which used the 2nd disk information of the above at least and can reproduce. Here, it has the key information record section which records the key information for decoding preferably the data which were enciphered and were recorded in the user data area.

[0255] In the above operation gestalt, the approach of recording the data of contents The 1st information field where the 1st disk information is recorded preferably, The 2nd information field where the 2nd disk information for identifying each disk is recorded, By irradiating a light beam, the user data area which can record informational, The optical disk which has the key information record section which records the key information for decoding the contents which were enciphered and were recorded in the above-mentioned user data area, In case contents are recorded on the above-mentioned user data area, it enciphers and records so that it may decode by the operation which used the 2nd disk information of the above, and the above-mentioned key information at least and can reproduce.

[0256] In the above operation gestalt, the size of the data which contain AV data preferably in the sector of the optical disk which has the decode key field which records two or more division decode keys divided into two or more continuous sectors records dummy data on the Maine data area with which x (the Maine data size) (number of partitions of a decode key) is not filled. Moreover, in an ECC block, only a (ECC block unit) / (number of partitions of a decode key) time is recorded, and the sector which has the decode key field which recorded the division decode key preferably divided into two or more continuous sectors records dummy data on the Maine data area with which the size of the data containing AV data does not fill x (the Maine data size) (ECC block unit).

[0257] In the above operation gestalt, the decode key for decoding the code given to the data containing AV data is preferably divided into two or more division decode keys which have predetermined size, and two or more divided division decode keys are recorded on two or more decode key fields to which a decode key table continues. Moreover, the above-mentioned decode key table is preferably recorded on the Maine data area in a rewritable lead-in groove field. Furthermore, the information showing the record condition of a decode key table is preferably recorded on each decode key field of a decode key table as a fixed value. Furthermore, only multiple times are recorded on the different above-mentioned ECC block with which the decode key table has been arranged at the inner circumference and the periphery of an optical disk.

[0258] In the above operation gestalt, the encoding equipment 3101 which is data encryption equipment, and the optical disk unit 3102 which is an optical disk record regenerative apparatus share a bus key with a mutual recognition method preferably.

Moreover, the optical disk unit 3102 which is the decoding equipment 3103 and the optical disk record regenerative apparatus which are data decryption equipment shares a bus key with a mutual recognition method preferably.

[0259] In the above operation gestalt, although this invention can read not only this but the data recorded beforehand although the record mold optical disk which can record the data which are the optical disk of the erasable type containing a RAM mold or a postscript mold is explained, and it can reproduce, it is applicable to the newly unrecordable mold optical disk only for playbacks. In the case of the mold optical disk only for playbacks, a data-logging playback field is replaced with the data playback field which reads and reproduces data, and the data of contents and the data of other various control information are beforehand recorded at the time of manufacture. Here, a record mold optical disk contains CD-R, CD-RW, MO and MD, DVD-RAM, etc. The mold optical disk only for playbacks contains Music CD, CD-ROM, DVD-ROM, etc.

[0260]

[Effect of the Invention] As explained in full detail above, according to the optical disk concerning this invention, the record actuation and playback actuation of contents of up to the optical disk by the user are controllable using the information recorded at the time of manufacture of an optical disk by being recorded on the field only for playbacks which cannot rewrite the disk identification information which performs record actuation to a user data area, and playback actuation for every optical disk.

[0261] Moreover, when the data enciphered as a key record the disk identification information only for playbacks which is not rewritable on the user data area on an optical disk, even if it copies to other record mold optical disks of the user data area by the user according to the optical disk concerning this invention, disk identification information cannot be copied but playback can be made impossible at the right decode list of data.

[0262] Furthermore, according to the optical disk concerning this invention, it becomes possible to acquire independently the descrambling key for solving acquisition and code of the data which need protection of copyrights, such as a film and music, by being recorded on the sector field to which the enciphered data differ from the descrambling key which solves a code. Furthermore, by enciphering and recording a descrambling key by using disk identification information as a key Even if it copies to other record mold optical disks of the user data area by the user Disk identification information cannot be copied, but playback can be made impossible at the right decode list of data, and playback can be made possible at the right decode list of data by acquiring and recording the descrambling key which enciphered the disk identification information of

the optical disk of a copy place as a key.

[0263] Moreover, according to the optical disk concerning this invention, it has the user data area which can record informational the 1st information field where the 1st disk information is recorded, the 2nd information field where the 2nd disk information for identifying each disk is recorded, and by irradiating a light beam. Therefore, management of an optical disk is easily realizable by adding the information which identifies the above-mentioned optical disk to the optical disk of the conventional technique. Here, preferably, the information field of the above 2nd is recorded in the information field of the above 1st, and can be reproduced by the optical pickup which reproduces the information field of the above 1st. Moreover, the information field of the above 2nd is recorded by removing selectively the record film in the information field of the above 1st so that it may be a long configuration and two or more trimming fields may be formed radially, and can prevent that the 2nd disk information of the above is altered easily.

[0264] Furthermore, according to the optical disk concerning this invention, a decode key is divided and recorded on the decode key field of the predetermined size arranged to the sector header field. Or by recording a variable-length decode key on the decode key field shown in the key index area arranged to the sector header field The record mold optical disk which can use the decode key of free die length can be offered without being caught by the decode key field of the size beforehand specified to the sector header field. Thereby, according to the protection-of-copyrights level to the contents to record, the code using the key length of arbitration can be made available.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the top view showing the data storage area of the record mold optical disk 100 which is the 1st operation gestalt concerning this invention.

[Drawing 2] (a) is the block diagram and drawing of longitudinal section showing the equipment configuration when forming BCA106 of the optical disk 100 of drawing 1 , and (b) is a graph which shows drawing of longitudinal section of the optical disk 100 after forming BCA106 of the optical disk 100 of drawing 1 , and the reinforcement of the reflected light which receives horizontally.

[Drawing 3] It is drawing showing a record format of drawing 1 of BCA106.

[Drawing 4] It is drawing showing the sector structure of the sector data 401 in the user

data area 102 of drawing 1 .

[Drawing 5] It is drawing showing the configuration of the key management information field 107 of drawing 1 .

[Drawing 6] (a) is the block diagram concerning the modification of the 1st operation gestalt showing the record approach which records a descrambling key and AV data to the sector data 401 of drawing 1 , and (b) is the block diagram concerning the 1st operation gestalt showing the record approach which records the key index and AV data to a descrambling key to the sector data 401 of drawing 1 .

[Drawing 7] It is the block diagram showing the configuration of the optical disk record regenerative apparatus which is the 2nd operation gestalt concerning this invention.

[Drawing 8] It is the flow chart which shows record processing of AV data performed by the control CPU 710 of the optical disk record regenerative apparatus of drawing 7 .

[Drawing 9] It is the flow chart which shows quota processing of the key management information field performed by the control CPU 710 of the optical disk record regenerative apparatus of drawing 7 .

[Drawing 10] It is the flow chart which shows record processing of the descrambling key performed by the control CPU 710 of the optical disk record regenerative apparatus of drawing 7 .

[Drawing 11] It is the flow chart which shows regeneration of AV data performed by the control CPU 710 of the optical disk record regenerative apparatus of drawing 7 .

[Drawing 12] It is the flow chart which shows acquisition processing of the descrambling key performed by the control CPU 710 of the optical disk record regenerative apparatus of drawing 7 .

[Drawing 13] It is the block diagram showing the approach for judging whether it is the descrambling key of normal from the encryption descrambling key concerning the modification of the 1st operation gestalt.

[Drawing 14] It is drawing concerning the modification of the 1st operation gestalt showing the configuration of a descrambling field managed table.

[Drawing 15] When recording a local identifier in the 1st operation gestalt at the time of record of contents, (a) in the same area Are drawing showing whether the copy and playback of contents are possible in an area which is different in a list, and when the local identifier is beforehand recorded in the 1st operation gestalt at the time of shipment of an optical disk, (b) in the same area It is an area which is different in a list, and is drawing showing whether the copy and playback of contents are possible.

[Drawing 16] It is the top view showing the data storage area of the optical disk 1101 which is the 3rd operation gestalt concerning this invention.

[Drawing 17] It is the wave form chart showing the signal wave form of the regenerative signal 1201 in the BCA regenerative circuit 1401 concerning the 3rd operation gestalt, and the playback binary-ized signal 1207.

[Drawing 18] It is the block diagram showing the configuration of the BCA regenerative circuit 1401 concerning the 3rd operation gestalt.

[Drawing 19] It is the block diagram showing the optical disk record playback structure of a system concerning the 3rd operation gestalt.

[Drawing 20] It is the block diagram showing the optical disk record playback structure of a system which is the 4th operation gestalt concerning this invention.

[Drawing 21] It is the top view showing the data storage area of the optical disk 1601 which is the 5th operation gestalt concerning this invention.

[Drawing 22] It is the block diagram showing the optical disk record playback structure of a system concerning the 5th operation gestalt.

[Drawing 23] It is the table showing the configuration of ID grant table concerning the 5th operation gestalt.

[Drawing 24] It is the top view showing the data storage area of optical disk 1101a concerning the modification of the 3rd operation gestalt.

[Drawing 25] It is the top view showing the data storage area of optical disk 1601a concerning the modification of the 5th operation gestalt.

[Drawing 26] It is the block diagram showing the configuration of the user data area in the optical disk which is the 6th operation gestalt concerning this invention, and the configuration of the optical disk regenerative apparatus which decodes encryption contents from the data of a user data area.

[Drawing 27] In the optical disk concerning the 6th operation gestalt, it is the block diagram showing the copyright control information to a user data area, arrangement of a decode key, and arrangement of the encryption contents to the Maine data area.

[Drawing 28] In the optical disk concerning the 6th operation gestalt, it is the block diagram showing arrangement in case the unit of an error correction straddles two or more sectors.

[Drawing 29] It is the block diagram showing the configuration of the lead-in groove field 2401 in the optical disk which is the 7th operation gestalt concerning this invention, and the user data area 2402, and the configuration of the optical disk regenerative apparatus which decodes encryption contents from the data of the lead-in groove field 2401 and the user data area 2402.

[Drawing 30] (a) is the block diagram showing the data configuration in the case of displaying the condition do not record, with the initial value of a decode key in the

Maine data area of the lead-in groove field in the optical disk concerning the 7th operation gestalt, and (b) is the block diagram showing the data configuration in the case of displaying a record condition on a decode key condition table in the Maine data area of the lead-in groove field in the optical disk concerning the 7th operation gestalt.

[Drawing 31] It is the block diagram showing arrangement of a decode key in the optical disk concerning the 7th operation gestalt.

[Drawing 32] It is the block diagram showing the data configuration when managing the data of the optical disk which is the 8th operation gestalt concerning this invention with file management system.

[Drawing 33] It is the flow chart which shows the record processing of contents which is performed by the file management system concerning the 8th operation gestalt, and which needs protection of copyrights.

[Drawing 34] It is the flow chart which is performed by the file management system concerning the 8th operation gestalt and which shows regeneration of contents.

[Drawing 35] It is the flow chart which is performed by the file management system concerning the 8th operation gestalt and which shows the deletion of contents.

[Drawing 36] It is the block diagram showing the configuration of the optical disc system which is the 9th operation gestalt concerning this invention.

[Drawing 37] It is the block diagram showing the configuration of the user data area in the optical disk which is the 10th operation gestalt concerning this invention, the configuration of the optical disk recording apparatus which carries out the code of the contents and is recorded on a user data area, and the configuration of the optical disk regenerative apparatus which decodes encryption contents from the data of a user data area.

[Drawing 38] It is the block diagram showing the configuration of the user data area in the optical disk which is the 11th operation gestalt concerning this invention, the configuration of the optical disk recording apparatus which carries out the code of the contents and is recorded on a user data area, and the configuration of the optical disk regenerative apparatus which decodes encryption contents from the data of a user data area.

[Drawing 39] It is the block diagram showing the configuration of the user data area of DVD-ROM of the conventional technique, and the configuration of the optical disk regenerative apparatus which decodes encryption contents from the data of a user data area.

[Description of Notations]

100 -- Optical disk

101 -- Lead-in groove field,
102 -- User data area,
103 -- Lead-out field,
104 -- Field only for playbacks,
105 -- Record playback field,
106 -- Burst cutting field (BCA),
107 -- Key management information field,
201 -- Substrate,
202 -- Recording layer,
203 -- Reflecting layer,
204 -- Glue line,
205 -- Reflecting layer,
206 -- Recording layer,
207 -- Substrate,
211 -- High-power laser light source,
212 -- Focal lens,
301 -- Synchronous code,
302 -- Error detecting code
303 -- Error correcting code
304 -- BCA data,
305 -- Disk identification information,
401 -- Sector data,
402 -- Header,
403 -- Maine data,
404 -- Error detection code
405 -- Data ID
406 -- ID error detection code,
407 -- Scramble control information,
408,408a -- Key information,
501 -- Key information field,
502 -- Contents information field,
503 -- Key-index list field,
504 -- The number of recorded keys,
505 -- Descrambling key area,
506 -- Key status field,
507 -- The number of contents,

508 -- Contents information,
509 -- Key index,
701 -- Record mold optical disk,
702 -- Optical head,
703 -- Record playback control circuit,
704 -- Strange demodulator circuit,
705 -- Error detection and correction circuit,
706 -- Buffer memory,
707 -- Descrambling circuit,
708 -- MPEG decoder circuit,
709 -- Output circuit,
710 -- Control CPU
711 -- Communication circuit,
712 -- Data receiving circuit,
801 -- Encryption descrambling key,
802 -- Descrambling key,
803 -- Error detecting code
1101 1101a -- Optical disk
1102 -- Control user data area,
1103 -- User data area,
1104, 1104 a--BCA,
1105 1105a -- Trimming field,
1201 -- Regenerative signal,
1202 thru/or 1204 -- Trimming part,
1205 1206 -- Slice level,
1207 -- Playback binary-ized signal,
1301 -- Optical pickup
1302 -- Pre amplifier,
1303 -- Low pass filter (LPF),
1304 -- Binary-ized circuit,
1305 -- Demodulator circuit,
1306 -- Disk ID signal,
1401 -- BCA regenerative circuit
1402 -- Disk ID signal,
1403 1404 -- Interface,
1405 -- Network,

1406 -- Encryption section,
1407 -- Contents memory,
1408 -- Encryption encoder,
1409 -- Encryption contents,
1410 -- Optical disk record regenerative apparatus,
1411 -- Record circuit,
1412 -- Data playback section,
1413 -- Code decoder,
1414 -- Output signal,
1501 -- CATV firm equipment,
1502 -- Contents memory,
1503 -- The 1st cryptographic key memory,
1504 -- The 1st encryption encoder,
1505 -- The 1st encryption contents,
1506 -- CATV decoder,
1507 -- Key issuance pin center,large equipment,
1507a -- Control section,
1508 -- System ID memory,
1509 -- Inputted title code,
1510 -- Time limit information memory,
1511 -- Record authorization code memory,
1512 -- Key (K),
1513 -- The 1st code decoder,
1514 -- Optical disk record regenerative apparatus,
1515 -- Disk ID signal,
1516 -- The 2nd encryption encoder,
1517 -- The 2nd encryption contents,
1518 -- Record circuit,
1519 -- Data playback section,
1520 -- The 2nd code decoder,
1521 -- BCA regenerative circuit,
1522 -- IC card
1523 -- Firm recognition signal memory,
1524 -- IC card
1525 -- Output signal,
1526 -- Firm recognition signal memory,

1527 -- Clock circuit,
1530 -- TV apparatus
1601 1601a -- Optical disk
1602 -- Control user data area,
1603 -- User data area,
1604, 1604 a--BCA,
1605 -- Key information record section,
1606 1606a -- Trimming field,
1701 -- CATV firm equipment,
1702 -- Contents memory,
1703 -- The 1st cryptographic key,
1704 -- The 1st encryption encoder,
1705 -- Key (K),
1706 -- CATV decoder,
1707 -- Key issuance pin center,large equipment,
1707a -- Control section,
1708 -- System ID memory,
1709 -- Inputted title code,
1710 -- Time limit information memory,
1712 -- Key (K),
1713 -- The 1st encryption decoder,
1714 -- Optical disk record regenerative apparatus,
1715 -- Disk ID
1716 -- Inputted title code,
1717 -- Record circuit,
1718 -- Key (DK),
1719 -- Key information record circuit,
1720 -- BCA regenerative circuit,
1721 -- Data playback section,
1722 -- The 2nd code decoder,
1723 -- Key information playback section,
1724 -- Output signal,
1725 -- Clock circuit,
1730 -- TV apparatus
2101 -- Sector header field,
2102 -- Maine data area,

2103 -- Error detecting code
2104 -- Sector address,
2105 -- Copyright control information,
2106 -- Decode key field,
2107 -- Non-enciphering contents,
2108 -- Encryption contents,
2109 -- Decode key field,
2110 -- Decode key translation data,
2111 -- Data coupler,
2112 -- Key decoder,
2113 -- Key converter,
2114 -- Decoder,
2115 -- 1st decode key translation data,
2116 -- 2nd decode key translation data,
2117 -- Non-enciphering control information,
2118 -- Key code machine,
2119 -- Key converter,
2120 -- Code machine,
2121 -- Data divider,
2150 -- User data area,
2151 -- Control information record sector,
2152 -- AV data-logging sector,
2201 -- 1st decode key field,
2202 -- 2nd decode key field,
2203 -- Complement data,
2204 -- Encryption contents,
2401 -- Lead-in groove field,
2402 -- User data area,
2403 -- Key index area,
2404 -- Decode key table,
2451 -- Control information record sector,
2452 -- AV data-logging sector,
2501 -- Condition [of not recording] data,
2502 -- Decode key condition table,
2503 -- Record condition data,
2601 -- Lead-in groove field,

2602 -- User data area,
2603 -- Lead-out field,
2701 -- File entry (1),
2702 -- File entry (2),
2703 -- File (1),
2704 -- File (2),
2705 -- Extent of a file (1) (1),
2706 -- Extent of a file (2) (1),
2707 -- Decode key table,
2708 -- Key index area,
2751 -- File management information field,
3101 -- Encoding equipment,
3102 -- Optical disk unit
3103 -- Decoding equipment,
3104 -- Personal computer,
3111 -- Decode key memory,
3112 -- Bus code circuit,
3113 -- Decode key table memory,
3114 -- A bus code and decoder circuit,
3115 -- Bus encryption decode key table memory,
3116 -- Decode key condition table memory,
3117 -- Bus decoder circuit,
3118 -- Decode key memory,
3119 -- Record regenerative circuit,
3120, 3121, 3123, 3124 -- Interface,
3130 -- Control section,
3131 -- Contents memory,
3132 -- Coding network,
3133 -- Cryptographic key memory,
3134 -- Code circuit,
3141 -- Decryption circuit,
3151 -- PCI bus
3152 -- SCSI bus.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－189015
（P2001－189015A）
(43)公開日　平成13年７月10日(2001.7.10)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
G11B	7/004		G11B	7/004	C　5D029
	7/24	522		7/24	522Z　5D044
		538			538P　5D066
					538G　5D090
		571			571A　5J104

審査請求　未請求　請求項の数73　ＯＬ　（全 57 頁）　最終頁に続く

(21)出願番号　特願2000－125933(P2000－125933)
(22)出願日　平成12年４月26日(2000.4.26)
(31)優先権主張番号　特願平11－122104
(32)優先日　平成11年４月28日(1999.4.28)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平11－128197
(32)優先日　平成11年５月10日(1999.5.10)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平11－299635
(32)優先日　平成11年10月21日(1999.10.21)
(33)優先権主張国　日本（ＪＰ）

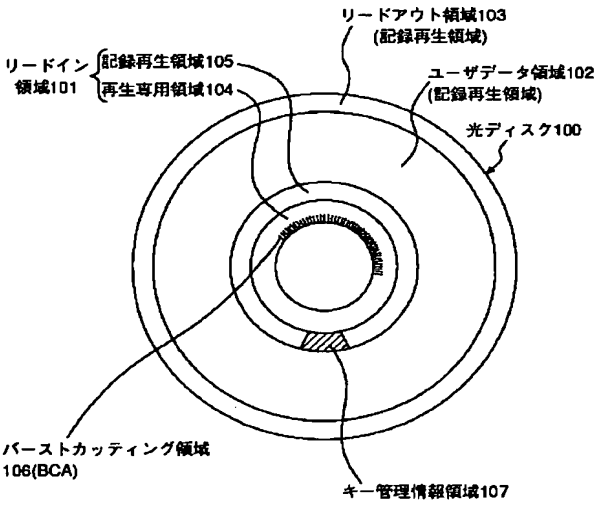
(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　永井　隆弘
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　石原　秀志
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100062144
弁理士　青山　葆　（外２名）

最終頁に続く

(54)【発明の名称】　光ディスク、光ディスク記録装置、光ディスク再生装置、光ディスク記録再生装置、光ディスク記録再生方法、光ディスク記録方法、光ディスク再生方法、光ディスク削除方法及び情報処理シ

(57)【要約】
【課題】　記録型光ディスクから他の記録型光ディスクへの不正なディジタルコピーを防止する。
【解決手段】　データを記録することができる記録型光ディスクにおいて、データを記録して再生するデータ記録再生領域と、上記光ディスクを識別するためのディスク識別情報を記録する再生専用のディスク識別情報領域とを含む。上記ディスク識別情報は、上記光ディスク上の反射膜をストライプ状に除去することにより形成される。上記ディスク識別情報は、各光ディスク毎に固有なディスク識別子を含む。また、上記データ記録再生領域は、上記光ディスクを識別するためのディスク識別情報を含む情報を鍵として用いて暗号化されたデータを記録する領域を含む。

第1の実施形態



【特許請求の範囲】

【請求項１】　データを記録することができる記録型光ディスクにおいて、

データを記録して再生するデータ記録再生領域と、

上記光ディスクを識別するためのディスク識別情報を記録する再生専用のディスク識別情報領域とを含むことを特徴とする光ディスク。

【請求項２】　上記ディスク識別情報は、上記光ディスク上の反射膜をストライプ状に除去することにより形成されたことを特徴とする請求項１記載の光ディスク。

【請求項３】　上記ディスク識別情報は、各光ディスク毎に固有なディスク識別子を含むことを特徴とする請求項１記載の光ディスク。

【請求項４】　上記データ記録再生領域は、上記光ディスクを識別するためのディスク識別情報を含む情報を鍵として用いて暗号化されたデータを記録する領域を含むことを特徴とする請求項１記載の光ディスク。

【請求項５】　上記暗号化されたデータは、画像データと音楽データとのうちの少なくとも一方であるコンテンツのデータを含むことを特徴とする請求項４記載の光ディスク。

【請求項６】　上記暗号化されたデータは、コンテンツのデータに施された暗号を解くためのデスクランブルキーを含むことを特徴とする請求項４又は５記載の光ディスク。

【請求項７】　上記暗号化されたデータは、コンテンツのデータに施された暗号を解くためのデスクランブルキーと、上記デスクランブルキーの誤りを検出するための誤り検出コードとを含むことを特徴とする請求項４又は５記載の光ディスク。

【請求項８】　データを記録することができる記録型光ディスクにおいて、

上記光ディスクは、データを記録して再生するデータ記録再生領域を含み、

上記データ記録再生領域は、暗号化された画像データと暗号化された音楽データとのうちの少なくとも一方であるコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを記録する領域を含むことを特徴とする光ディスク。

【請求項９】　上記コンテンツのデータと、上記デスクランブルキーは、同一のセクタ内に記録されたことを特徴とする請求項８記載の光ディスク。

【請求項１０】　上記コンテンツのデータと、上記デスクランブルキーは異なるセクタに記録されたことを特徴とする請求項８記載の光ディスク。

【請求項１１】　上記コンテンツが記録されたセクタに、上記デスクランブルキーが記録される領域を示すポインタを記録したことを特徴とする請求項１０記載の光ディスク。

【請求項１２】　データを記録することができる記録型光ディスクにおいて、

上記光ディスクを識別するためのディスク識別情報を記録する再生専用のディスク識別情報領域と、

暗号化された画像データと、暗号化された音楽データとのうちの少なくとも一方を含むコンテンツのデータを記録して再生するデータ記録再生領域と、

上記コンテンツのデータを再生するときに使用するキー情報と、上記ディスク識別情報を鍵として用いて暗号化されたデスクランブルキーとを記録するキー管理情報領域とを含むことを特徴とする光ディスク。

【請求項１３】　データを記録することができる記録型光ディスクのデータ記録再生領域に対してデータを記録する記録動作と、上記データ記録再生領域からデータを再生する再生動作とのうちの少なくとも一方を制御する光ディスク記録再生装置であって、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記ディスク識別情報領域から上記ディスク識別情報を再生する再生手段と、

上記再生されたディスク識別情報に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するか否かを判断し、当該判断結果に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するように制御する制御手段とを備えたことを特徴とする光ディスク記録再生装置。

【請求項１４】　データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録装置において、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記ディスク識別情報領域からディスク識別情報を再生する再生手段と、

上記再生されたディスク識別情報を鍵として用いて、少なくとも一部が暗号化されたデータを上記光ディスクに対して記録する記録手段とを備えたことを特徴とする光ディスク記録装置。

【請求項１５】　上記暗号化されたデータは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーを含むことを特徴とする請求項１４記載の光ディスク記録装置。

【請求項１６】　上記暗号化されたデータは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーと、上記デスクランブルキーの誤りを検出するための誤り検出コードとを含むことを特徴とする請求項１４記載の光ディスク記録装置。

【請求項１７】　データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生装置において、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、
上記ディスク識別情報領域からディスク識別情報を再生する再生手段と、少なくとも一部が暗号化されたデータを上記光ディスクから再生した後、上記再生されたディスク識別情報を鍵として用いて復号化する復号化手段とを備えたことを特徴とする光ディスク再生装置。
【請求項１８】　上記復号化されるデータは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーを含むことを特徴とする請求項１７記載の光ディスク再生装置。
【請求項１９】　上記復号化されるデータは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーと、上記デスクランブルキーの誤りを検出するための誤り検出コードとを含み、
上記復号化手段は、上記デスクランブルキーに含まれる誤りを、上記誤り検出コードに基づいて検出することを特徴とする請求項１７記載の光ディスク再生装置。
【請求項２０】　データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録装置において、
暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを上記光ディスクに記録する記録手段を備えたことを特徴とする光ディスク記録装置。
【請求項２１】　上記記録手段は、上記暗号化されたコンテンツのデータを所定の第１のセクタに記録し、上記デスクランブルキーを上記第１のセクタとは異なる第２のセクタに記録することを特徴とする請求項２０記載の光ディスク記録装置。
【請求項２２】　上記記録手段は、上記暗号化されたコンテンツのデータが記録された第１のセクタに、上記デスクランブルキーが記録された第２のセクタ内の領域を示すポインタを記録することを特徴とする請求項２１記載の光ディスク記録装置。
【請求項２３】　データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生装置において、
暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを、上記光ディスクから再生する再生手段を備えたことを特徴とする光ディスク再生装置。
【請求項２４】　上記再生手段は、上記暗号化されたコンテンツを上記光ディスクの第１のセクタから再生し、上記デスクランブルキーを上記第１のセクタとは異なる第２のセクタから再生することを特徴とする請求項２３記載の光ディスク再生装置。
【請求項２５】　上記再生手段は、上記暗号化されたコンテンツのデータが記録された第１のセクタから、上記デスクランブルキーが再生される第２のセクタ内の領域を示すポインタを再生することを特徴とする請求項２４記載の光ディスク再生装置。
【請求項２６】　データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を割り当てて記録する光ディスク記録装置であって、
記録すべきコンテンツのデータに必要なデスクランブルキーに関する情報を取得する取得手段と、
上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報と、上記取得されたデスクランブルキーに関する情報とに基づいて、記録すべきデスクランブルキーを記録する領域を上記キー管理情報領域内で割り当てる割当手段とを備えたことを特徴とする光ディスク記録装置。
【請求項２７】　データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を記録する光ディスク記録装置であって、
コンテンツのデータを再生するために必要なデスクランブルキーを取得する取得手段と、
上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報に基づいて、上記取得されたデスクランブルキーを上記キー管理情報領域内で配置するように記録する記録手段とを備えたことを特徴とする光ディスク記録装置。
【請求項２８】　データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録装置において、
上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、
上記ディスク識別情報領域からディスク識別情報を再生する再生手段と、
上記再生されたディスク識別情報に基づいて、コンテンツのデータを上記光ディスクに記録することができるか否かを判断する判断手段と、
上記コンテンツのデータを上記光ディスクに記録することができると判断されたときに、上記コンテンツのデータを暗号化するために必要なデスクランブルキーを記録するための領域を、上記光ディスク内のキー管理情報領域において割り当てる割当手段と、
記録すべきコンテンツのデータのデスクランブルキーを記録する領域を示すキーインデックスを、上記記録すべきコンテンツのデータが記録されたセクタと同一のセクタに記録する記録手段とを備えたことを特徴とする光ディスク記録装置。
【請求項２９】　データを記録することができる記録型光ディスクのキー管理情報領域から、デスクランブルキーを再生する光ディスク再生装置であって、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、
上記キー管理情報領域のデータを再生する第１の再生手段と、
上記再生されたキー管理情報領域内のセクタ領域のデータに基づいて、上記セクタ領域のデータがスクランブルされているか否かを判断する判断手段と、
上記セクタ領域のデータがスクランブルされていると判断されたときに、上記セクタ領域のデータが記録されたセクタ領域と同一のセクタ領域内に記録されているキーインデックスを再生し、上記再生されたキーインデックスで示されるデスクランブルキー領域からデスクランブルキーを再生する第２の再生手段と、
上記ディスク識別情報領域からディスク識別情報を再生する第３の再生手段と、
上記再生されたディスク識別情報を鍵として用いて、上記再生された暗号化されたデスクランブルキーを復号化することにより再生する復号化手段とを備えたことを特徴とする光ディスク再生装置。

【請求項３０】　上記復号化されたデスクランブルキーに、誤り検出コードが付与され、上記復号化手段は、上記復号化されたデスクランブルキーに付与された誤り検出コードに基づいて、上記復号化されたデスクランブルキーにおける誤りの有無を判断し、上記判断結果に基づいて、上記復号化されたデスクランブルキーを再生するか否かを判断することを特徴とする請求項２９記載の光ディスク再生装置。

【請求項３１】　データを記録することができる記録型光ディスクのデータ記録再生領域に対してデータを記録する記録動作と、上記データ記録再生領域からデータを再生する再生動作とのうちの少なくとも一方を制御する光ディスク記録再生方法であって、
上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、
上記ディスク識別情報領域から上記ディスク識別情報を再生するステップと、
上記再生されたディスク識別情報に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するか否かを判断し、当該判断結果に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するように制御するステップとを含むことを特徴とする光ディスク記録再生方法。

【請求項３２】　データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録方法において、
上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、
上記ディスク識別情報領域からディスク識別情報を再生するステップと、
上記再生されたディスク識別情報を鍵として用いて、少なくとも一部が暗号化されたデータを上記光ディスクに対して記録するステップとを含むことを特徴とする光ディスク記録方法。

【請求項３３】　データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生方法において、
上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、
上記ディスク識別情報領域からディスク識別情報を再生するステップと、
少なくとも一部が暗号化されたデータを上記光ディスクから再生した後、上記再生されたディスク識別情報を鍵として用いて復号化するステップとを含むことを特徴とする光ディスク再生方法。

【請求項３４】　データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録方法において、
暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを上記光ディスクに記録するステップを含むことを特徴とする光ディスク記録方法。

【請求項３５】　データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生方法において、
暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを、上記光ディスクから再生するステップを含むことを特徴とする光ディスク再生方法。

【請求項３６】　データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を割り当てて記録する光ディスク記録方法であって、
記録すべきコンテンツのデータに必要なデスクランブルキーに関する情報を取得するステップと、
上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報と、上記取得されたデスクランブルキーに関する情報とに基づいて、記録すべきデスクランブルキーを記録する領域を上記キー管理情報領域内で割り当てるステップとを含むことを特徴とする光ディスク記録方法。

【請求項３７】　データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を記録する光ディスク記録方法であって、
コンテンツのデータを再生するために必要なデスクランブルキーを取得するステップと、

上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報に基づいて、上記取得されたデスクランブルキーを上記キー管理情報領域内で配置するように記録するステップとを含むことを特徴とする光ディスク記録方法。

【請求項３８】　データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録方法において、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記ディスク識別情報領域からディスク識別情報を再生するステップと、

上記再生されたディスク識別情報に基づいて、コンテンツのデータを上記光ディスクに記録することができるか否かを判断するステップと、

上記コンテンツのデータを上記光ディスクに記録することができると判断されたときに、上記コンテンツのデータを暗号化するために必要なデスクランブルキーを記録するための領域を、上記光ディスク内のキー管理情報領域において割り当てるステップと、

記録すべきコンテンツのデータのデスクランブルキーを記録する領域を示すキーインデックスを、上記記録すべきコンテンツのデータが記録されたセクタと同一のセクタに記録するステップとを含むことを特徴とする光ディスク記録方法。

【請求項３９】　データを記録することができる記録型光ディスクのキー管理情報領域から、デスクランブルキーを再生する光ディスク再生方法であって、

上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、

上記キー管理情報領域のデータを再生するステップと、

上記再生されたキー管理情報領域内のセクタ領域のデータに基づいて、上記セクタ領域のデータがスクランブルされているか否かを判断するステップと、

上記セクタ領域のデータがスクランブルされていると判断されたときに、上記セクタ領域のデータが記録されたセクタ領域と同一のセクタ領域内に記録されているキーインデックスを再生し、上記再生されたキーインデックスで示されるデスクランブルキー領域からデスクランブルキーを再生するステップと、

上記ディスク識別情報領域からディスク識別情報を再生するステップと、

上記再生されたディスク識別情報を鍵として用いて、上記再生された暗号化されたデスクランブルキーを復号化することにより再生するステップとを含むことを特徴とする光ディスク再生方法。

【請求項４０】　データを記録することができる記録型光ディスクにおいて、

第１のディスク情報を記録する第１の情報領域と、

各光ディスクを識別するための第２のディスク情報を記録する第２の情報領域と、

光ビームを当該領域に照射することにより情報データを記録するユーザデータ領域とを含むことを特徴とする光ディスク。

【請求項４１】　上記第２のディスク情報は、上記第２の情報領域内の記録膜を、半径方向に長い形状でかつ複数個の領域において部分的に除去することにより記録されたことを特徴とする請求項４０記載の光ディスク。

【請求項４２】　上記第２の情報領域は、上記第１の情報領域内に配置されたことを特徴とする請求項４０又は４１記載の光ディスク。

【請求項４３】　上記第２の情報領域は、上記第１の情報領域の内周側に配置されたことを特徴とする請求項４０又は４１記載の光ディスク。

【請求項４４】　上記第２の情報領域は、上記第１の情報領域内の一部の領域と、上記第１の情報領域よりも内周側に位置する別の領域とにわたって配置されたことを特徴とする請求項４０又は４１記載の光ディスク。

【請求項４５】　上記第１のディスク情報は、微少な凹凸ピットの形式で記録されたことを特徴とする請求項４０乃至４４のうちの１つに記載の光ディスク。

【請求項４６】　データを記録することができる記録型光ディスクにおいて、

上記光ディスクは、複数のセクタを備えたセクタ構造を有し、

上記各セクタは、セクタヘッダ領域と、暗号化されたデータを記録するメインデータ領域とを含み、

上記セクタヘッダ領域は、上記暗号化されたデータを復号化するために必要な少なくとも１つの復号鍵を記録する復号鍵情報領域を含み、

上記復号鍵情報領域のサイズは上記各復号鍵のサイズよりも小さいことを特徴とする光ディスク。

【請求項４７】　上記各復号鍵は、所定のサイズを有する複数の分割復号鍵に分割され、

上記複数の分割復号鍵は、連続する複数のセクタの各復号鍵情報領域に記録されたことを特徴とする請求項４６記載の光ディスク。

【請求項４８】　上記復号鍵の分割数は、エラー訂正に必要な複数のセクタである誤り訂正コード（ＥＣＣ）ブロックに含まれるセクタ数の約数であることを特徴とする請求項４７記載の光ディスク。

【請求項４９】　上記各復号鍵は、複数の復号鍵を有する復号鍵テーブルに記録され、

上記暗号化されたデータを復号化するために必要な復号鍵の、上記復号鍵テーブル内の記録位置を示すインデックスは、上記セクタの復号鍵情報領域に記録されたことを特徴とする請求項４６記載の光ディスク。

【請求項５０】　上記復号鍵テーブルの記録状態を表す

情報として、上記復号鍵テーブルの各復号鍵領域に対する復号鍵状態を記録した復号鍵状態領域が記録された請求項４９記載の光ディスク。

【請求項５１】　上記復号鍵テーブルは、異なる複数の誤り訂正コード（ＥＣＣ）ブロックにわたって記録されたことを特徴とする請求項４９記載の光ディスク。

【請求項５２】　上記各復号鍵は、ファイル管理領域で管理されるファイル単位と、光ディスク上で連続する複数のセクタからなるエクステント単位とのうちの少なくとも一方の単位で管理されて記録されたことを特徴とする請求項４９９記載の光ディスク。

【請求項５３】　データを記録することができる記録型光ディスクにおいて、
上記光ディスクは、データを記録するメインデータ領域を含み、
上記メインデータ領域は、データを非暗号化状態で記録する非暗号化領域と、データを暗号化状態で記録する暗号化領域とを含み、
上記非暗号化領域は、データを復号化するための復号鍵の変換に用いられる復号鍵変換データを含み、
上記暗号化領域のデータは、上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化されていることを特徴とする光ディスク。

【請求項５４】　上記メインデータ領域は、データの再生制御のために用いられる制御情報を非暗号化状態で記録する制御情報記録セクタと、データを暗号化状態で記録するデータ記録セクタとを含み、
上記制御情報記録セクタは、上記復号鍵の変換のために用いられる復号鍵変換データを含み、
上記データ記録セクタのデータは上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化されていることを特徴とする請求項５３記載の光ディスク。

【請求項５５】　上記データ記録セクタは、データを非暗号化状態で記録する非暗号化領域と、データを暗号化状態で記録する暗号化領域とを含み、
上記非暗号化領域は別の復号鍵変換データを含み、
上記暗号化領域のＡＶデータは上記復号鍵変換データを用いて変換された復号鍵をさらに別の第２の復号鍵変換データを用いて変換された復号鍵を用いて暗号化されていることを特徴とする請求項５４記載の光ディスク。

【請求項５６】　上記復号鍵変換データは、少なくともデータのコピー制御情報を含むことを特徴とする請求項５３記載の光ディスク。

【請求項５７】　データを記録することができる記録型光ディスクにデータを記録するための光ディスク記録方法において、
上記光ディスク上に記録された復号鍵ステータスを読み出し、上記読み出された復号鍵ステータスに基づいて復号鍵の空き領域があるか否かを判断するステップと、
上記復号鍵の空き領域があると判断されたときに、復号鍵領域を予約して復号鍵を記録するステップと、
ファイル単位とエクステント単位のうちの少なくとも一方の単位で著作権制御情報と復号鍵インデックスを設定するステップと、
上記復号鍵を用いてデータを暗号化して、暗号化されたデータを、ファイル単位とエクステント単位のうちの少なくとも一方の単位で上記光ディスクに記録するステップと、
上記光ディスクに記録されたデータを管理するためのファイル管理情報を上記光ディスクに記録するステップとを含むことを特徴とする光ディスク記録方法。

【請求項５８】　データを記録することができる記録型光ディスクからデータを再生するための光ディスク再生方法において、
ファイル単位又はエクステント単位で記録された再生すべきデータの記録領域から復号鍵インデックスを再生して取得するステップと、
上記取得された復号鍵インデックスに対応する復号鍵を再生して取得するステップと、
上記復号鍵を用いて暗号化されたファイル単位又はエクステント単位のデータを再生するステップとを含むことを特徴とする光ディスク再生方法。

【請求項５９】　データを記録することができる記録型光ディスクからデータを削除するための光ディスク削除方法において、
ファイル単位又はエクステント単位で記録された削除すべきデータの記録領域から復号鍵インデックスを再生して取得するステップと、
上記取得された復号鍵インデックスに対応し、復号鍵の記録状態を示す復号鍵ステータスを更新して復号鍵を開放するステップと、
上記光ディスクに記録されたデータを管理するためのファイル管理情報から上記削除すべきデータに対応するファイルエントリを削除することにより上記ファイル管理情報を更新するステップとを含むことを特徴とする光ディスク削除方法。

【請求項６０】　データを暗号鍵を用いて暗号化するデータ暗号化装置と、
上記データを復号化するために必要な復号鍵を記録型光ディスクに記録して再生する光ディスク記録再生装置と、
上記光ディスク記録再生装置及び上記データ暗号化装置に接続された制御装置とを備えた情報処理システムであって、
上記光ディスク記録再生装置は、
上記光ディスクに復号鍵テーブルを記録し、上記光ディスクから復号鍵テーブルを再生する第１の記録再生手段と、
上記復号鍵を暗号化して上記制御装置に送信し、上記制御装置から暗号化された復号鍵を受信して復号化する暗

号化及び復号化手段と、
上記光ディスクに復号鍵の記録状態を示す復号鍵状態テーブルを記録し、上記光ディスクから復号鍵状態テーブルを再生する第２の記録再生手段とを備え、
上記データ暗号化装置は、
上記復号鍵を暗号化して上記制御装置に送信する暗号化手段を備え、
上記制御装置は、
上記データ暗号化装置の暗号化手段から暗号化された復号鍵を受信する受信手段と、
上記再生された復号鍵状態テーブルに基づいて復号鍵の空き領域を検索し、上記検索された空き領域に、上記受信された暗号化された復号鍵を割り当て、上記割り当てられた暗号化された復号鍵を上記光ディスク記録再生装置に送信する割当手段とを備え、
上記光ディスク記録再生装置の暗号化及び復号化手段は、上記制御装置の割当手段から上記割り当てられた暗号化された復号鍵を受信して復号化することを特徴とする情報処理システム。

【請求項６１】　データと、上記データを復号化するために必要な複数の復号鍵を備えた復号鍵テーブルを記録型光ディスクから再生する光ディスク再生装置と、
上記光ディスク再生装置に接続された制御装置と、
復号鍵を用いてデータを復号化するデータ復号化装置とを備えた情報処理システムであって、
上記光ディスク再生装置は、
上記光ディスクから復号鍵テーブルを再生する第１の再生手段と、
上記再生された復号鍵テーブルを暗号化して、暗号化された復号鍵テーブルを上記制御装置に送信する暗号化手段と、
上記光ディスクから複数の復号鍵の記録状態を示す復号鍵状態テーブルを再生する第２の再生手段とを備え、
上記制御装置は、
上記光ディスク再生装置から上記暗号化された復号鍵テーブルを受信する受信手段と、
上記再生された復号鍵状態テーブルに基づいて、上記受信された復号鍵テーブルから上記光ディスクに記録されたデータを復号化するために必要な暗号化された復号鍵を検索して上記データ復号化手段に送信する検索手段とを備え、
上記データ復号化装置は、
上記暗号化された復号鍵を復号化して復号鍵を生成する第１の復号化手段と、
光ディスク再生装置によって再生された暗号化されたデータを、上記復号化された復号鍵を用いて復号化する第２の復号化手段とを備えたことを特徴とする情報処理システム。

【請求項６２】　データを記録することができる記録型光ディスクにデータを記録する光ディスク記録装置において、
上記光ディスクは、非暗号化領域と、暗号化領域とを含み、
データを復号化するための復号鍵の変換に用いられる復号鍵変換データを含むデータを非暗号化状態で上記非暗号化領域に記録し、上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化されたデータを上記暗号化領域に記録する記録手段を備えたことを特徴とする光ディスク記録装置。

【請求項６３】　上記光ディスクは、制御情報記録セクタと、データ記録セクタとを含み、
上記記録手段は、上記データの再生制御のために用いられる制御情報を上記制御情報記録セクタに非暗号化状態で記録し、上記制御情報に含まれる復号鍵変換データを用いて暗号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いてデータを暗号化して上記データ記録セクタに記録することを特徴とする請求項６２記載の光ディスク記録装置。

【請求項６４】　上記記録手段は、別の復号鍵変換データを含むデータを非暗号化状態で上記データ記録セクタの非暗号化領域に記録し、上記制御情報に含まれる復号鍵変換データと、上記別の復号鍵変換データとを用いて暗号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いてデータを暗号化して上記データ記録セクタに記録することを特徴とする請求項６３記載の光ディスク記録装置。

【請求項６５】　データを記録することができる記録型光ディスクからデータを再生する光ディスク再生装置において、
上記光ディスクは、非暗号化領域と、暗号化領域とを含み、
上記非暗号化領域に記録された復号鍵変換データを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記暗号化領域に記録されたデータを復号化して再生する再生手段を備えたことを特徴とする光ディスク再生装置。

【請求項６６】　上記光ディスクは、制御情報記録セクタと、データ記録セクタとを含み、
上記再生手段は、上記データの再生制御のために用いられる制御情報を制御情報記録セクタから再生し、上記制御情報に含まれる復号鍵変換データを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記データ記録セクタに記録されたデータを復号化して再生することを特徴とする請求項６５記載の光ディスク再生装置。

【請求項６７】　上記再生手段は、上記データ記録セクタの非暗号化領域に記録された別の復号鍵変換データを再生し、上記制御情報に含まれる復号鍵変換データと、上記再生された別の復号鍵変換データとを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を

用いて上記データ記録セクタに記録されたデータを復号化して再生することを特徴とする請求項６６記載の光ディスク再生装置。

【請求項６８】　データを記録することができる記録型光ディスクにデータを記録する光ディスク記録方法において、

上記光ディスクは、非暗号化領域と、暗号化領域とを含み、

データを復号化するための復号鍵の変換に用いられる復号鍵変換データを含むデータを非暗号化状態で上記非暗号化領域に記録し、上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化されたデータを上記暗号化領域に記録するステップを含むことを特徴とする光ディスク記録方法。

【請求項６９】　データを記録することができる記録型光ディスクからデータを再生する光ディスク再生方法において、

上記光ディスクは、非暗号化領域と、暗号化領域とを含み、

上記非暗号化領域に記録された復号鍵変換データを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記暗号化領域に記録されたデータを復号化して再生するステップを含むことを特徴とする光ディスク再生方法。

【請求項７０】　記録されたデータを再生するための再生専用型光ディスクにおいて、

データが記録されたデータ再生領域と、

上記光ディスクを識別するためのディスク識別情報が記録された再生専用のディスク識別情報領域とを含み、

上記データ再生領域は、上記光ディスクを識別するためのディスク識別情報を含む情報を鍵として用いて暗号化されたデータが記録された領域を含むことを特徴とする光ディスク。

【請求項７１】　記録されたデータを再生するための再生専用型光ディスクにおいて、

上記光ディスクは、データが記録されたデータ再生領域を含み、

上記データ再生領域は、暗号化された画像データと暗号化された音楽データとのうちの少なくとも一方であるコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとが記録された領域を含むことを特徴とする光ディスク。

【請求項７２】　記録されたデータを再生するための再生専用型光ディスクにおいて、

上記光ディスクを識別するためのディスク識別情報が記録された再生専用のディスク識別情報領域と、

暗号化された画像データと、暗号化された音楽データとのうちの少なくとも一方を含むコンテンツのデータが記録されたデータ再生領域と、

上記コンテンツのデータを再生するときに使用するキー情報と、上記ディスク識別情報を鍵として用いて暗号化されたデスクランブルキーとが記録されたキー管理情報領域とを含むことを特徴とする光ディスク。

【請求項７３】　記録されたデータを再生するための再生専用型光ディスクにおいて、

上記光ディスクは、複数のセクタを備えたセクタ構造を有し、

上記各セクタは、セクタヘッダ領域と、暗号化されたデータが記録されたメインデータ領域とを含み、

上記セクタヘッダ領域は、上記暗号化されたデータを復号化するために必要な少なくとも１つの復号鍵が記録された復号鍵情報領域を含み、

上記復号鍵情報領域のサイズは上記各復号鍵のサイズよりも小さいことを特徴とする光ディスク。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、著作権を有する映画の画像データや音楽の音声データを含むＡＶデータ（Audio and Visual Data）などのデータが記録されている光ディスクから、他の記録型光ディスクなどの記録媒体への不正なディジタルコピーを防止することができる、光ディスク、光ディスク記録装置、光ディスク再生装置、光ディスク記録再生装置、光ディスク記録再生方法、光ディスク記録方法、光ディスク再生方法、光ディスク削除方法、及び情報処理システムに関する。

【０００２】

【従来の技術】光ディスクは、従来のテープメディアに比べてランダムアクセス性に優れており、また、レーザ光を利用した非接触な記録及び再生が可能なため繰り返し利用による劣化が少ないという特徴を有している。さらに、光ディスクは、ディスク製造者によるマスタリングによって、安価に大量の複製が可能という特徴を有しており、高音質のディジタルオーディオとしてＣＤ（Compact Disk）が従来のアナログ記録のレコードにとって代わって一般的になっている。さらに、近年、高品質の画像データがディジタル記録されたＤＶＤ（Digital Video Disk、又はDigital Versatile Disk）が商品化されＡＶデータのディジタル記録媒体としての光ディスクが今後さらに発展していくことが予想される。

【０００３】一方、音楽ＣＤ、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭのように、ディスク製造業者によってデータがプリピットの形式で予め記録されている再生専用の光ディスクだけでなく、近年、ユーザが家庭でＡＶデータを記録できる、例えば、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＭＯ、ＭＤやＤＶＤ－ＲＡＭなどの記録型の光ディスクが開発され、世に広がりつつある。

【０００４】また、テレビ放送においても従来のアナログ方式から多チャンネル化や様々なサービスが可能なディジタル方式が導入されており、このような傾向は今後さらに広がっていく。特に、記録型光ディスクは、ディ

ジタル化された放送や通信で配信されてくるコンテンツの記録媒体として、配信時に蓄積した後プログラム選択して視聴するタイムシフト利用を目的の中心としたＡＶデータの記録に利用されることが予想される。

【０００５】従来、コンピュータを中心に利用されてきた記録型の光ディスクは、利用者自らが作成したデータの保存を目的として利用されており、記録型の光ディスク間でのコピーを制限する仕組みを有していなかった。記録型の光ディスクが広く利用されるようになると、記録された光ディスクのデータを、一般ユーザがそのまま他の記録型光ディスクに違法にコピーすることにより、本来そのＡＶデータの著作者に支払われるべき著作料を払うこと無しに、また、ディジタル記録が可能なことから音質や画質の劣化なしに不当な複製を入手することが可能になり、良質のコンテンツの広まりを阻害する要因にもなってきている。音楽等をディジタル記録するＭＤでは、記録回数を制限する世代管理を行う仕組みが導入され、世代管理データとともに光ディスクに記録し、その世代管理データによりコピー回数の制限を行っている。

【０００６】また、例えば、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭの不正なコピーを防止するために、光ディスクのピット部にバーコードを重ね書きするための追記領域であるバーストカッティング領域（Burst Cutting Area；以下、ＢＣＡという。）を設け、光ディスクの製造時にＢＣＡにディスク毎に異なるＩＤを記録しておく方法が、国際公開番号ＷＯ９７／１４１４４号の国際出願において提案されている。この方法によると、パスワードはディスクＩＤにより異なるので、１つのパスワードは１枚のディスクの暗号しか解読することができなくなり、コンテンツが不正にコピーされてもディスクＩＤの情報が欠落しているため、コンテンツは解読されなくなる。

【０００７】図３９は、従来技術のＤＶＤ－ＲＯＭのユーザデータ領域の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。ＤＶＤ－ＲＯＭでは、図３９に示すように、ディスク上に記録するコンテンツのデータに対して暗号化を行っている。

【０００８】図３９において、ＤＶＤ－ＲＯＭのユーザデータ領域は、セクタヘッダ領域３２０１と、メインデータ領域３２０２と、誤り検出コード３２０３とから構成される。ここで、セクタヘッダ領域３２０１には、セクタの位置を示すセクタアドレス３２０４と、メインデータ領域３２０２に記録されるデータに関する著作権制御情報（例えば、スクランブルフラグ、コピー制御情報など）が記録される著作権制御情報３２０５と、メインデータ領域３２０２のデータに暗号が施されている場合に復号するための復号鍵３２０６とが記録される。また、メインデータ領域３２０２には、主に著作権保護を必要とするＡＶデータなどが暗号化されて記録される。

【０００９】このようなユーザデータ領域の再生時には、まず、セクタヘッダ領域３２０１から暗号化コンテンツの再生に必要な復号鍵３２０６を得る。取得した復号鍵３２０６は鍵復号器３２０７に入力され、鍵復号器３２０７は入力された復号鍵３２０６を所定のディスク鍵を用いてコンテンツ復号鍵を復号して、復号器３２０８に出力する。次いで、復号器３２０８は、メインデータ領域３２０２に対応するセクタヘッダ領域３２０１に格納された著作権制御情報３２０５に従って、メインデータ領域３２０２の暗号化コンテンツを上記復号されたコンテンツ復号鍵を用いて復号を行い、再生可能なデータである復号化コンテンツを得る。

【００１０】図３９に示した構成による光ディスクでは、パーソナルコンピュータのドライブ装置などからメインデータ領域３２０２に対する読み出しが可能であるが、復号鍵３２０６を記録した領域を正規の認証機能を有する光ディスク再生装置しか読み出しできないように構成することにより、不正な複製や海賊版の作成を防止できるようにしている。

【００１１】

【発明が解決しようとする課題】しかしながら、世代管理データを用いた不正コピー防止方法では、コピー時に世代管理データの変更（“１回コピー可能”から“コピー不可”への情報の変更“）が不可欠である。これに対して、光ディスク上のデータを世代管理データとともに変更を加えずコピーしたり、コンピュータ等で世代管理データを改ざんして記録したりすることにより、不正コピーを十分に防止できないという問題点を有していた。さらに、コンテンツとともに予め記録した世代管理データによりコピー回数の制限を行うため、たとえ正規の著作料を払ったとしても光ディスク上の“コピー不可”となったデータは他の光ディスクへのコピーが全く許されず、利用者はコンテンツ供給者から供給を待たなければならないという問題を有していた。いずれもコンテンツ供給者が利用者の行う記録型光ディスクへのコピーを十分に管理できないことによるものである。

【００１２】近年、パーソナルコンピュータが高性能化し、さらにそれらがネットワークに接続されることによって、高性能でかつ、複数台のパーソナルコンピュータによる高速な暗号の解読が行われている。このような解読に対して、より暗号の強度を高めるためには、暗号に使用する鍵の鍵長を拡張することが必要となる。しかしながら、従来から提案されているようなセクタヘッダに復号鍵を記録するような鍵管理方法では、予め決められた長さ（復号鍵領域のサイズ）以下の復号鍵しか記録することができず、将来に暗号の強度を高めるために鍵長を長くできないという問題点があった。

【００１３】本発明の第１の目的は、以上の問題点を解決し、コンテンツ供給者が管理できない不正なディジタルコピーを防止できる、光ディスク、光ディスク記録装

置、光ディスク再生装置、光ディスク記録再生装置、光ディスク記録再生方法、光ディスク記録方法、光ディスク再生方法、光ディスク削除方法及び情報処理システムを提供することにある。

【００１４】また、本発明の第２の目的は、以上の問題点を解決し、著作権保護を必要とするデータを復号化するために必要な復号鍵の信頼性をより高めることができる、光ディスク、光ディスク記録装置、光ディスク再生装置、光ディスク記録再生装置、光ディスク記録再生方法、光ディスク記録方法、光ディスク再生方法、光ディスク削除方法及び情報処理システムを提供することにある。

【００１５】さらに、本発明の第３の目的は、以上の問題点を解決し、記録するコンテンツの著作権保護のレベルに応じて暗号強度の設定することができる、光ディスク、光ディスク記録装置、光ディスク再生装置、光ディスク記録再生装置、光ディスク記録再生方法、光ディスク記録方法、光ディスク再生方法、光ディスク削除方法及び情報処理システムを提供することにある。

【００１６】

【課題を解決するための手段】本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、データを記録して再生するデータ記録再生領域と、上記光ディスクを識別するためのディスク識別情報を記録する再生専用のディスク識別情報領域とを含むことを特徴とする。

【００１７】上記光ディスクにおいて、上記ディスク識別情報は、好ましくは、上記光ディスク上の反射膜をストライプ状に除去することにより形成される。また、上記光ディスクにおいて、上記ディスク識別情報は、好ましくは、各光ディスク毎に固有なディスク識別子を含む。

【００１８】また、上記光ディスクにおいて、上記データ記録再生領域は、好ましくは、上記光ディスクを識別するためのディスク識別情報を含む情報を鍵として用いて暗号化されたデータを記録する領域を含む。上記光ディスクにおいて、上記暗号化されたデータは、好ましくは、画像データと音楽データとのうちの少なくとも一方であるコンテンツのデータを含む。また、上記光ディスクにおいて、上記暗号化されたデータは、好ましくは、コンテンツのデータに施された暗号を解くためのデスクランブルキーを含む。さらに、上記光ディスクにおいて、上記暗号化されたデータは、好ましくは、コンテンツのデータに施された暗号を解くためのデスクランブルキーと、上記デスクランブルキーの誤りを検出するための誤り検出コードとを含む。

【００１９】本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、上記光ディスクは、データを記録して再生するデータ記録再生領域を含み、上記データ記録再生領域は、暗号化された画像データと暗号化された音楽データとのうちの少なくとも一方であるコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを記録する領域を含むことを特徴とする。

【００２０】上記光ディスクにおいて、好ましくは、上記コンテンツのデータと、上記デスクランブルキーは、同一のセクタ内に記録され、もしくは、上記コンテンツのデータと、上記デスクランブルキーは異なるセクタに記録される。また、上記光ディスクにおいて、好ましくは、上記コンテンツが記録されたセクタに、上記デスクランブルキーが記録される領域を示すポインタを記録する。

【００２１】本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、上記光ディスクを識別するためのディスク識別情報を記録する再生専用のディスク識別情報領域と、暗号化された画像データと、暗号化された音楽データとのうちの少なくとも一方を含むコンテンツのデータを記録して再生するデータ記録再生領域と、上記コンテンツのデータを再生するときに使用するキー情報と、上記ディスク識別情報を鍵として用いて暗号化されたデスクランブルキーとを記録するキー管理情報領域とを含むことを特徴とする。

【００２２】本発明に係る光ディスク記録再生装置は、データを記録することができる記録型光ディスクのデータ記録再生領域に対してデータを記録する記録動作と、上記データ記録再生領域からデータを再生する再生動作とのうちの少なくとも一方を制御する光ディスク記録再生装置であって、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記ディスク識別情報領域から上記ディスク識別情報を再生する再生手段と、上記再生されたディスク識別情報に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するか否かを判断し、当該判断結果に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するように制御する制御手段とを備えたことを特徴とする。

【００２３】本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録装置において、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記ディスク識別情報領域からディスク識別情報を再生する再生手段と、上記再生されたディスク識別情報を鍵として用いて、少なくとも一部が暗号化されたデータを上記光ディスクに対して記録する記録手段とを備えたことを特徴とする。

【００２４】上記光ディスク記録装置において、上記暗号化されたデータは、好ましくは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーを含む。また、上記光ディスク記録装置において、上記暗

号化されたデータは、好ましくは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーと、上記デスクランブルキーの誤りを検出するための誤り検出コードとを含む。

【００２５】本発明に係る光ディスク再生装置は、データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生装置において、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記ディスク識別情報領域からディスク識別情報を再生する再生手段と、少なくとも一部が暗号化されたデータを上記光ディスクから再生した後、上記再生されたディスク識別情報を鍵として用いて復号化する復号化手段とを備えたことを特徴とする。

【００２６】上記光ディスク再生装置において、上記復号化されるデータは、好ましくは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーを含む。また、光ディスク再生装置において、上記復号化されるデータは、好ましくは、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーと、上記デスクランブルキーの誤りを検出するための誤り検出コードとを含み、上記復号化手段は、上記デスクランブルキーに含まれる誤りを、上記誤り検出コードに基づいて検出する。

【００２７】本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録装置において、暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを上記光ディスクに記録する記録手段を備えたことを特徴とする。

【００２８】上記光ディスク記録装置において、上記記録手段は、好ましくは、上記暗号化されたコンテンツのデータを所定の第１のセクタに記録し、上記デスクランブルキーを上記第１のセクタとは異なる第２のセクタに記録する。また、上記光ディスク記録装置において、上記記録手段は、好ましくは、上記暗号化されたコンテンツのデータが記録された第１のセクタに、上記デスクランブルキーが記録された第２のセクタ内の領域を示すポインタを記録する。

【００２９】本発明に係る光ディスク再生装置は、データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生装置において、暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを、上記光ディスクから再生する再生手段を備えたことを特徴とする。

【００３０】上記光ディスク再生装置において、上記再生手段は、好ましくは、上記暗号化されたコンテンツを上記光ディスクの第１のセクタから再生し、上記デスクランブルキーを上記第１のセクタとは異なる第２のセクタから再生する。上記光ディスク再生装置において、上記再生手段は、好ましくは、上記暗号化されたコンテンツのデータが記録された第１のセクタから、上記デスクランブルキーが再生される第２のセクタ内の領域を示すポインタを再生する。

【００３１】本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を割り当てて記録する光ディスク記録装置であって、記録すべきコンテンツのデータに必要なデスクランブルキーに関する情報を取得する取得手段と、上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報と、上記取得されたデスクランブルキーに関する情報とに基づいて、記録すべきデスクランブルキーを記録する領域を上記キー管理情報領域内で割り当てる割当手段とを備えたことを特徴とする。

【００３２】本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を記録する光ディスク記録装置であって、コンテンツのデータを再生するために必要なデスクランブルキーを取得する取得手段と、上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報に基づいて、上記取得されたデスクランブルキーを上記キー管理情報領域内で配置するように記録する記録手段とを備えたことを特徴とする。

【００３３】本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録装置において、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記ディスク識別情報領域からディスク識別情報を再生する再生手段と、上記再生されたディスク識別情報に基づいて、コンテンツのデータを上記光ディスクに記録することができるか否かを判断する判断手段と、上記コンテンツのデータを上記光ディスクに記録することができると判断されたときに、上記コンテンツのデータを暗号化するために必要なデスクランブルキーを記録するための領域を、上記光ディスク内のキー管理情報領域において割り当てる割当手段と、記録すべきコンテンツのデータのデスクランブルキーを記録する領域を示すキーインデックスを、上記記録すべきコンテンツのデータが記録されたセクタと同一のセクタに記録する記録手段とを備えたことを特徴とする。

【００３４】本発明に係る光ディスク再生装置は、データを記録することができる記録型光ディスクのキー管理情報領域から、デスクランブルキーを再生する光ディス

ク再生装置であって、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記キー管理情報領域のデータを再生する第１の再生手段と、上記再生されたキー管理情報領域内のセクタ領域のデータに基づいて、上記セクタ領域のデータがスクランブルされているか否かを判断する判断手段と、上記セクタ領域のデータがスクランブルされていると判断されたときに、上記セクタ領域のデータが記録されたセクタ領域と同一のセクタ領域内に記録されているキーインデックスを再生し、上記再生されたキーインデックスで示されるデスクランブルキー領域からデスクランブルキーを再生する第２の再生手段と、上記ディスク識別情報領域からディスク識別情報を再生する第３の再生手段と、上記再生されたディスク識別情報を鍵として用いて、上記再生された暗号化されたデスクランブルキーを復号化することにより再生する復号化手段とを備えたことを特徴とする。

【００３５】上記光ディスク再生装置において、好ましくは、上記復号化されたデスクランブルキーに、誤り検出コードが付与され、上記復号化手段は、上記復号化されたデスクランブルキーに付与された誤り検出コードに基づいて、上記復号化されたデスクランブルキーにおける誤りの有無を判断し、上記判断結果に基づいて、上記復号化されたデスクランブルキーを再生するか否かを判断する。

【００３６】本発明に係る光ディスク記録再生方法は、データを記録することができる記録型光ディスクのデータ記録再生領域に対してデータを記録する記録動作と、上記データ記録再生領域からデータを再生する再生動作とのうちの少なくとも一方を制御する光ディスク記録再生方法であって、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記ディスク識別情報領域から上記ディスク識別情報を再生するステップと、上記再生されたディスク識別情報に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するか否かを判断し、当該判断結果に基づいて、上記記録動作と、上記再生動作とのうちの少なくとも一方を実行するように制御するステップとを含むことを特徴とする。

【００３７】本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録方法において、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記ディスク識別情報領域からディスク識別情報を再生するステップと、上記再生されたディスク識別情報を鍵として用いて、少なくとも一部が暗号化されたデータを上記光ディスクに対して記録するステップとを含むことを特徴とする。

【００３８】本発明に係る光ディスク再生方法は、データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生方法において、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記ディスク識別情報領域からディスク識別情報を再生するステップと、少なくとも一部が暗号化されたデータを上記光ディスクから再生した後、上記再生されたディスク識別情報を鍵として用いて復号化するステップとを含むことを特徴とする。

【００３９】本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録方法において、暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを上記光ディスクに記録するステップを含むことを特徴とする。

【００４０】本発明に係る光ディスク再生方法は、データを記録することができる記録型光ディスクからコンテンツのデータを再生する光ディスク再生方法において、暗号化されたコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとを、上記光ディスクから再生するステップを含むことを特徴とする。

【００４１】本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を割り当てて記録する光ディスク記録方法であって、記録すべきコンテンツのデータに必要なデスクランブルキーに関する情報を取得するステップと、上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報と、上記取得されたデスクランブルキーに関する情報とに基づいて、記録すべきデスクランブルキーを記録する領域を上記キー管理情報領域内で割り当てるステップとを含むことを特徴とする。

【００４２】本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクのキー管理情報領域に、コンテンツのデータを暗号化するために必要なデスクランブルキーの情報を記録する光ディスク記録方法であって、コンテンツのデータを再生するために必要なデスクランブルキーを取得するステップと、上記キー管理情報領域に記録されたデスクランブルキーの情報を再生し、上記再生されたデスクランブルキーの情報に基づいて、上記取得されたデスクランブルキーを上記キー管理情報領域内で配置するように記録するステップとを含むことを特徴とする。

【００４３】本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクに対してコンテンツのデータを記録する光ディスク記録方法において、上記光ディスクは、上記光ディスクを識別するため

のディスク識別情報を記録するディスク識別情報領域を含み、上記ディスク識別情報領域からディスク識別情報を再生するステップと、上記再生されたディスク識別情報に基づいて、コンテンツのデータを上記光ディスクに記録することができるか否かを判断するステップと、上記コンテンツのデータを上記光ディスクに記録することができると判断されたときに、上記コンテンツのデータを暗号化するために必要なデスクランブルキーを記録するための領域を、上記光ディスク内のキー管理情報領域において割り当てるステップと、記録すべきコンテンツのデータのデスクランブルキーを記録する領域を示すキーインデックスを、上記記録すべきコンテンツのデータが記録されたセクタと同一のセクタに記録するステップとを含むことを特徴とする。

【００４４】本発明に係る光ディスク再生方法は、データを記録することができる記録型光ディスクのキー管理情報領域から、デスクランブルキーを再生する光ディスク再生方法であって、上記光ディスクは、上記光ディスクを識別するためのディスク識別情報を記録するディスク識別情報領域を含み、上記キー管理情報領域のデータを再生するステップと、上記再生されたキー管理情報領域内のセクタ領域のデータに基づいて、上記セクタ領域のデータがスクランブルされているか否かを判断するステップと、上記セクタ領域のデータがスクランブルされていると判断されたときに、上記セクタ領域のデータが記録されたセクタ領域と同一のセクタ領域内に記録されているキーインデックスを再生し、上記再生されたキーインデックスで示されるデスクランブルキー領域からデスクランブルキーを再生するステップと、上記ディスク識別情報領域からディスク識別情報を再生するステップと、上記再生されたディスク識別情報を鍵として用いて、上記再生された暗号化されたデスクランブルキーを復号化することにより再生するステップとを含むことを特徴とする。

【００４５】本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、第１のディスク情報を記録する第１の情報領域と、各光ディスクを識別するための第２のディスク情報を記録する第２の情報領域と、光ビームを当該領域に照射することにより情報データを記録するユーザデータ領域とを含むことを特徴とする。

【００４６】上記光ディスクにおいて、上記第２のディスク情報は、好ましくは、上記第２の情報領域内の記録膜を、半径方向に長い形状でかつ複数個の領域において部分的に除去することにより記録される。また、上記光ディスクにおいて、好ましくは、上記第２の情報領域は、上記第１の情報領域内に配置され、又は、上記第１の情報領域の内周側に配置され、もしくは、上記第２の情報領域は、上記第１の情報領域内の一部の領域と、上記第１の情報領域よりも内周側に位置する別の領域とにわたって配置される。さらに、上記第１のディスク情報は、好ましくは、微少な凹凸ピットの形式で記録される。

【００４７】本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、上記光ディスクは、複数のセクタを備えたセクタ構造を有し、上記各セクタは、セクタヘッダ領域と、暗号化されたデータを記録するメインデータ領域とを含み、上記セクタヘッダ領域は、上記暗号化されたデータを復号化するために必要な少なくとも１つの復号鍵を記録する復号鍵情報領域を含み、上記復号鍵情報領域のサイズは上記各復号鍵のサイズよりも小さいことを特徴とする。

【００４８】上記光ディスクにおいて、上記各復号鍵は、好ましくは、所定のサイズを有する複数の分割復号鍵に分割され、上記複数の分割復号鍵は、連続する複数のセクタの各復号鍵情報領域に記録される。ここで、上記復号鍵の分割数は、好ましくは、エラー訂正に必要な複数のセクタである誤り訂正コード（ＥＣＣ）ブロックに含まれるセクタ数の約数である。また、上記光ディスクにおいて、上記各復号鍵は、好ましくは、複数の復号鍵を有する復号鍵テーブルに記録され、上記暗号化されたデータを復号化するために必要な復号鍵の、上記復号鍵テーブル内の記録位置を示すインデックスは、上記セクタの復号鍵情報領域に記録される。さらに、上記光ディスクにおいて、上記復号鍵テーブルの記録状態を表す情報として、好ましくは、上記復号鍵テーブルの各復号鍵領域に対する復号鍵状態を記録した復号鍵状態領域が記録される。またさらに、上記光ディスクにおいて、上記復号鍵テーブルは、好ましくは、異なる複数の誤り訂正コード（ＥＣＣ）ブロックにわたって記録される。また、上記光ディスクにおいて、上記各復号鍵は、好ましくは、ファイル管理領域で管理されるファイル単位と、光ディスク上で連続する複数のセクタからなるエクステント単位とのうちの少なくとも一方の単位で管理されて記録される。

【００４９】本発明に係る光ディスクは、データを記録することができる記録型光ディスクにおいて、上記光ディスクは、データを記録するメインデータ領域を含み、上記メインデータ領域は、データを非暗号化状態で記録する非暗号化領域と、データを暗号化状態で記録する暗号化領域とを含み、上記非暗号化領域は、データを復号化するための復号鍵の変換に用いられる復号鍵変換データを含み、上記暗号化領域のデータは、上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化されていることを特徴とする。

【００５０】上記光ディスクにおいて、好ましくは、上記メインデータ領域は、データの再生制御のために用いられる制御情報を非暗号化状態で記録する制御情報記録セクタと、データを暗号化状態で記録するデータ記録セクタとを含み、上記制御情報記録セクタは、上記復号鍵

の変換のために用いられる復号鍵変換データを含み、上記データ記録セクタのデータは上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化される。また、上記光ディスクにおいて、好ましくは、上記データ記録セクタは、データを非暗号化状態で記録する非暗号化領域と、データを暗号化状態で記録する暗号化領域とを含み、上記非暗号化領域は別の復号鍵変換データを含み、上記暗号化領域のＡＶデータは上記復号鍵変換データを用いて変換された復号鍵をさらに別の第２の復号鍵変換データを用いて変換された復号鍵を用いて暗号化される。さらに、上記光ディスクにおいて、上記復号鍵変換データは、好ましくは、少なくともデータのコピー制御情報を含む。

【００５１】本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクにデータを記録するための光ディスク記録方法において、上記光ディスク上に記録された復号鍵ステータスを読み出し、上記読み出された復号鍵ステータスに基づいて復号鍵の空き領域があるか否かを判断するステップと、上記復号鍵の空き領域があると判断されたときに、復号鍵領域を予約して復号鍵を記録するステップと、ファイル単位とエクステント単位のうちの少なくとも一方の単位で著作権制御情報と復号鍵インデックスを設定するステップと、上記復号鍵を用いてデータを暗号化して、暗号化されたデータを、ファイル単位とエクステント単位のうちの少なくとも一方の単位で上記光ディスクに記録するステップと、上記光ディスクに記録されたデータを管理するためのファイル管理情報を上記光ディスクに記録するステップとを含むことを特徴とする。

【００５２】本発明に係る光ディスク再生方法は、データを記録することができる記録型光ディスクからデータを再生するための光ディスク再生方法において、ファイル単位又はエクステント単位で記録された再生すべきデータの記録領域から復号鍵インデックスを再生して取得するステップと、上記取得された復号鍵インデックスに対応する復号鍵を再生して取得するステップと、上記復号鍵を用いて暗号化されたファイル単位又はエクステント単位のデータを再生するステップとを含むことを特徴とする。

【００５３】本発明に係る光ディスク削除方法は、データを記録することができる記録型光ディスクからデータを削除するための光ディスク削除方法において、ファイル単位又はエクステント単位で記録された削除すべきデータの記録領域から復号鍵インデックスを再生して取得するステップと、上記取得された復号鍵インデックスに対応し、復号鍵の記録状態を示す復号鍵ステータスを更新して復号鍵を開放するステップと、上記光ディスクに記録されたデータを管理するためのファイル管理情報から上記削除すべきデータに対応するファイルエントリを削除することにより上記ファイル管理情報を更新するステップとを含むことを特徴とする。

【００５４】本発明に係る情報処理システムは、データを暗号鍵を用いて暗号化するデータ暗号化装置と、上記データを復号化するために必要な復号鍵を記録型光ディスクに記録して再生する光ディスク記録再生装置と、上記光ディスク記録再生装置及び上記データ暗号化装置に接続された制御装置とを備えた情報処理システムであって、上記光ディスク記録再生装置は、上記光ディスクに復号鍵テーブルを記録し、上記光ディスクから復号鍵テーブルを再生する第１の記録再生手段と、上記復号鍵を暗号化して上記制御装置に送信し、上記制御装置から暗号化された復号鍵を受信して復号化する暗号化及び復号化手段と、上記光ディスクに復号鍵の記録状態を示す復号鍵状態テーブルを記録し、上記光ディスクから復号鍵状態テーブルを再生する第２の記録再生手段とを備え、上記データ暗号化装置は、上記復号鍵を暗号化して上記制御装置に送信する暗号化手段を備え、上記制御装置は、上記データ暗号化装置の暗号化手段から暗号化された復号鍵を受信する受信手段と、上記再生された復号鍵状態テーブルに基づいて復号鍵の空き領域を検索し、上記検索された空き領域に、上記受信された暗号化された復号鍵を割り当て、上記割り当てられた暗号化された復号鍵を上記光ディスク記録再生装置に送信する割当手段とを備え、上記光ディスク記録再生装置の暗号化及び復号化手段は、上記制御装置の割当手段から上記割り当てられた暗号化された復号鍵を受信して復号化することを特徴とする。

【００５５】本発明に係る情報処理システムは、データと、上記データを復号化するために必要な複数の復号鍵を備えた復号鍵テーブルを記録型光ディスクから再生する光ディスク再生装置と、上記光ディスク再生装置に接続された制御装置と、復号鍵を用いてデータを復号化するデータ復号化装置とを備えた情報処理システムであって、上記光ディスク再生装置は、上記光ディスクから復号鍵テーブルを再生する第１の再生手段と、上記再生された復号鍵テーブルを暗号化して、暗号化された復号鍵テーブルを上記制御装置に送信する暗号化手段と、上記光ディスクから複数の復号鍵の記録状態を示す復号鍵状態テーブルを再生する第２の再生手段とを備え、上記制御装置は、上記光ディスク再生装置から上記暗号化された復号鍵テーブルを受信する受信手段と、上記再生された復号鍵状態テーブルに基づいて、上記受信された復号鍵テーブルから上記光ディスクに記録されたデータを復号化するために必要な暗号化された復号鍵を検索して上記データ復号化手段に送信する検索手段とを備え、上記データ復号化装置は、上記暗号化された復号鍵を復号化して復号鍵を生成する第１の復号化手段と、光ディスク再生装置によって再生された暗号化されたデータを、上記復号化された復号鍵を用いて復号化する第２の復号化手段とを備えたことを特徴とする。

【００５６】本発明に係る光ディスク記録装置は、データを記録することができる記録型光ディスクにデータを記録する光ディスク記録装置において、上記光ディスクは、非暗号化領域と、暗号化領域とを含み、データを復号化するための復号鍵の変換に用いられる復号鍵変換データを含むデータを非暗号化状態で上記非暗号化領域に記録し、上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化されたデータを上記暗号化領域に記録する記録手段を備えたことを特徴とする。

【００５７】上記光ディスク記録装置において、好ましくは、上記光ディスクは、制御情報記録セクタと、データ記録セクタとを含み、上記記録手段は、上記データの再生制御のために用いられる制御情報を上記制御情報記録セクタに非暗号化状態で記録し、上記制御情報に含まれる復号鍵変換データを用いて暗号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いてデータを暗号化して上記データ記録セクタに記録する。また、上記光ディスク記録装置において、上記記録手段は、好ましくは、別の復号鍵変換データを含むデータを非暗号化状態で上記データ記録セクタの非暗号化領域に記録し、上記制御情報に含まれる復号鍵変換データと、上記別の復号鍵変換データとを用いて暗号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いてデータを暗号化して上記データ記録セクタに記録する。

【００５８】本発明に係る光ディスク再生装置は、データを記録することができる記録型光ディスクからデータを再生する光ディスク再生装置において、上記光ディスクは、非暗号化領域と、暗号化領域とを含み、上記非暗号化領域に記録された復号鍵変換データを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記暗号化領域に記録されたデータを復号化して再生する再生手段を備えたことを特徴とする。

【００５９】上記光ディスク再生装置において、好ましくは、上記光ディスクは、制御情報記録セクタと、データ記録セクタとを含み、上記再生手段は、上記データの再生制御のために用いられる制御情報を制御情報記録セクタから再生し、上記制御情報に含まれる復号鍵変換データを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記データ記録セクタに記録されたデータを復号化して再生する。また、上記光ディスク再生装置において、上記再生手段は、好ましくは、上記データ記録セクタの非暗号化領域に記録された別の復号鍵変換データを再生し、上記制御情報に含まれる復号鍵変換データと、上記再生された別の復号鍵変換データとを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記データ記録セクタに記録されたデータを復号化して再生する。

【００６０】本発明に係る光ディスク記録方法は、データを記録することができる記録型光ディスクにデータを記録する光ディスク記録方法において、上記光ディスクは、非暗号化領域と、暗号化領域とを含み、データを復号化するための復号鍵の変換に用いられる復号鍵変換データを含むデータを非暗号化状態で上記非暗号化領域に記録し、上記復号鍵変換データを用いて変換された復号鍵を用いて暗号化されたデータを上記暗号化領域に記録するステップを含むことを特徴とする。

【００６１】本発明に係る光ディスク再生方法は、データを記録することができる記録型光ディスクからデータを再生する光ディスク再生方法において、上記光ディスクは、非暗号化領域と、暗号化領域とを含み、上記非暗号化領域に記録された復号鍵変換データを用いて復号鍵を変換された復号鍵に変換し、上記変換された復号鍵を用いて上記暗号化領域に記録されたデータを復号化して再生するステップを含むことを特徴とする。

【００６２】本発明に係る光ディスクは、記録されたデータを再生するための再生専用型光ディスクにおいて、データが記録されたデータ再生領域と、上記光ディスクを識別するためのディスク識別情報が記録された再生専用のディスク識別情報領域とを含み、上記データ再生領域は、上記光ディスクを識別するためのディスク識別情報を含む情報を鍵として用いて暗号化されたデータが記録された領域を含むことを特徴とする。

【００６３】本発明に係る光ディスクは、記録されたデータを再生するための再生専用型光ディスクにおいて、上記光ディスクは、データが記録されたデータ再生領域を含み、上記データ再生領域は、暗号化された画像データと暗号化された音楽データとのうちの少なくとも一方であるコンテンツのデータと、上記コンテンツのデータに施された暗号を解くためのデスクランブルキーとが記録された領域を含むことを特徴とする。

【００６４】本発明に係る光ディスクは、記録されたデータを再生するための再生専用型光ディスクにおいて、上記光ディスクを識別するためのディスク識別情報が記録された再生専用のディスク識別情報領域と、暗号化された画像データと、暗号化された音楽データとのうちの少なくとも一方を含むコンテンツのデータが記録されたデータ再生領域と、上記コンテンツのデータを再生するときに使用するキー情報と、上記ディスク識別情報を鍵として用いて暗号化されたデスクランブルキーとが記録されたキー管理情報領域とを含むことを特徴とする。

【００６５】本発明に係る光ディスクは、記録されたデータを再生するための再生専用型光ディスクにおいて、上記光ディスクは、複数のセクタを備えたセクタ構造を有し、上記各セクタは、セクタヘッダ領域と、暗号化されたデータが記録されたメインデータ領域とを含み、上記セクタヘッダ領域は、上記暗号化されたデータを復号化するために必要な少なくとも１つの復号鍵が記録された復号鍵情報領域を含み、上記復号鍵情報領域のサイズは上記各復号鍵のサイズよりも小さいことを特徴とする。

【００６６】
【発明の実施の形態】以下、図面を参照して本発明に係る実施形態について説明する。
【００６７】＜第１の実施形態＞図１は、本発明に係る第１の実施形態である記録型光ディスク１００のデータ記録領域を示す平面図である。この記録型光ディスク１００は、ディジタルデータを記録することが可能な記録媒体であって、追記型光ディスクと、書き換え型光ディスクを含む。
【００６８】図１において、１０１は光ディスク１００の管理情報が記録されたリードイン領域、１０２は映画などの画像データ（静止画及び動画を含む。）や音楽などの音声データの少なくとも一方を含むＡＶデータのコンテンツや、コンピュータのソフトウェアなどの、著作権保護が必要なディジタルデータが記録されるユーザデータ領域、１０３は欠陥管理情報等が記録されるリードアウト領域である。リードイン領域１０１は、プリピットの形で記録された再生専用領域１０４と、ガイド溝を有する書き換え可能領域である記録再生領域１０５により構成される。ここで、再生専用領域１０４には、光ディスク１００の物理特性を記述したコントロール領域などが製造業者によりプリピットの形式で記録される。リードアウト領域１０３や書き換え可能領域１０５には、光ディスク記録装置による書き込みテストのためのデータや光ディスク１００上の欠陥を管理するための管理情報などが光ディスク記録装置により記録される。さらに、リードイン領域１０１の再生専用領域１０４の内周側には、ディスク個別情報としてＢＣＡ１０６は、以下に示すように公知の方法で、コンテンツが記録された光ディスク１００が完成した後に、光ディスク１００に追記される。
【００６９】図２（ａ）は図１の光ディスク１００のＢＣＡ１０６を形成するときの装置構成を示すブロック図及び縦断面図であり、図２（ｂ）は図１の光ディスク１００のＢＣＡ１０６を形成した後の光ディスク１００の縦断面図及びその水平方向に対する反射光の強度を示すグラフである。図２（ａ）及び図２（ｂ）では、両面記録型の光ディスク１００の例を示しており、光ディスク１００は、２つの基板２０１，２０７の間に、記録層２０２、反射層２０３、接着層２０４、反射層２０５及び記録層２０６が挿入されて構成される。
【００７０】ＢＣＡを光ディスク１００に記録するときにおいては、図２（ａ）に示すように、高パワーレーザ光源２１１からのレーザ光をフォーカスレンズ２１２を介して、例えば光ディスク１００の反射層２０５にパルス状に照射して一部の反射層２０５を除去することにより、位相符号化変調（phase encoding modulation）したストライプ状のデータをピットに重ねて記録する。再生時には、図２（ｂ）に示すように、反射層２０５が除去されている部分で反射光量が低下した信号が断続的に再生され、再生された信号を２値化した後、位相符号化復調（phase encoding demodulation）することにより、ＢＣＡのデータを再生する。このような記録方式により作成されたＢＣＡは、各光ディスク１００毎に固有な情報であるディスク識別子を記録することができ、さらに改ざんすることが不可能であるなどの特徴を有する。
【００７１】図３は、図１のＢＣＡ１０６の記録フォーマットを示す図である。図３に示すように、ＢＣＡ１０６には、同期コード３０１、エラー検出コード３０２、エラー訂正コード３０３などがＢＣＡデータ３０４の読み取り率を改善するために記録される。これらの複数のＢＣＡデータ３０４を連結することによって、ディスク識別情報３０５が構成される。ディスク識別情報３０５には、ユーザデータ領域へ記録可能なデータの種別の種別、ユーザデータ領域から再生可能なデータの種別が記録される。ＢＣＡ１０６のデータは改ざんが不可能であるため、光ディスク１００の製造時に記録されるディスク識別情報により利用者のディスク使用に一定の制限を与えることができる。
【００７２】図４は、図１のユーザデータ領域１０２内のセクタデータ４０１のセクタ構造を示す図である。図４において、図１のユーザデータ領域１０２は、一定量の単位でアクセス可能なセクタ構造を有しており、そのセクタデータ４０１は、ヘッダ４０２、メインデータ４０３、エラー検出コード４０４により構成される。
【００７３】ここで、メインデータ４０３は、ＡＶデータやコンピュータのデータなどが記録される領域である。また、ヘッダ４０２には、データＩＤ（Data Identifier）４０５、ＩＤエラー検出コード４０６、スクランブル制御情報４０７、キー情報４０８などが記録される。データＩＤ４０５には、セクタを識別するための論理アドレスなどが記録され、ＩＤエラー検出コード４０６はデータＩＤのエラー検出するためのコードである。また、スクランブル制御情報４０７は、メインデータにスクランブルが施されているか否かを示すフラグであり、キー情報４０８はメインデータをデスクランブルするためのキーに関する情報が記録される。キーに関する情報としては、デスクランブルキーそのもの（第１の実施形態の変形例）や、光ディスク１００上の別領域に記録したデスクランブルキーへのポインタであるキーインデックス（第１の実施形態）が記録される。図４の例では、光ディスク１００上の別領域である図１のキー管理情報領域１０７に記録したデスクランブルキーを参照するためのキーインデックスが記録されている場合を示している。
【００７４】図５は、図１のキー管理情報領域１０７の構成を示す図である。図５において、キー管理情報領域１０７は、キー情報領域５０１と、コンテンツ情報領域５０２と、キーインデックスリスト領域５０３とから構

成される。

【００７５】キー情報領域５０１には、使用済みのデスクランブルキー領域の数５０４が記録されるとともに、キー情報領域５０１は、ＡＶデータ等に施されたスクランブルを解くためのデスクランブルキーを記録する領域であるデスクランブルキー領域５０５と、デスクランブルキー領域５０５に記録されるデスクランブルキーの記録状態（未使用、領域予約済、記録済などを示す。）を記録するキーステータス領域５０６とを含む。デスクランブルキー領域５０５には複数のデスクランブルキーが記録され、デスクランブルキー領域５０５中での格納位置を表すキーインデックスがキーインデックスリスト領域５０３に記録され、上記複数のデスクランブルキーは当該キーインデックスにより参照可能である。キーステータス領域５０６には、先のデスクランブルキーの記録状態を表すステータス情報がキーインデックスで参照可能な位置に格納される。

【００７６】コンテンツ情報領域５０２には、光ディスク１００上に記録されるコンテンツの中で著作権保護が必要なものが登録され、それとともにコンテンツで使用されるキーに関する情報が登録される。コンテンツ情報領域５０２は、キーインデックスリスト領域５０３に登録されるコンテンツ数５０７と、コンテンツ数分のコンテンツ情報５０８が記録される。さらに、コンテンツ情報５０８には、コンテンツを識別するためのコンテンツＩＤと、そのコンテンツで使用されるデスクランブルキーの個数と、使用するキーを記録したキーインデックスリスト５０９へのポインタが記録される。キーインデックスリスト領域５０３は、コンテンツで使用するキーを参照するためのインデックスをコンテンツ単位でのリスト形式で記録する領域である。キーインデックスリスト領域５０３には、コンテンツで使用されている全デスクランブルキーの記録領域を参照するキーインデックスが記録される。

【００７７】このように構成された記録型光ディスク１００では、書き換えが困難なディスク識別情報にディスクの使用条件を表すような情報として、地域識別子、データカテゴリ識別子、ディスク識別子などを製造時に記録することにより、光ディスク記録再生装置でこれらの情報を検出し、コンテンツが持つ著作権の保護レベルや利用レベルに応じて記録動作及び再生動作を制御することを可能とする。また、書き換えが困難な方法によって記録されており利用者の側での変更ができないため、別の光ディスクに著作権保護されたコンテンツをコピーした場合でも、ユーザデータ領域はコピー可能であるが、ディスク識別情報はコピーすることはできない。従って、ディスク識別情報を用いてスクランブルしたデータを光ディスク上に記録しておくことで、異なるディスク識別情報を有する光ディスクではデスクランブルできないユーザデータ領域が存在し正しい再生ができない。

【００７８】図１５（ａ）は第１の実施形態においてコンテンツの記録時に地域識別子を記録する場合に、同一の地域内で、並びに異なる地域で、コンテンツのコピーや再生が可能であるか否かを示す図であり、図１５（ｂ）は第１の実施形態において地域識別子が光ディスクの出荷時に予め記録されている場合に、同一の地域内で、並びに異なる地域で、コンテンツのコピーや再生が可能であるか否かを示す図である。

【００７９】例えば、図１５（ａ）に示すように、光ディスクの出荷時に地域識別コードが記録されておらず、コンテンツの記録時にコンテンツが利用可能な地域を表す地域識別子を記録及び再生領域に記録した場合には、他の地域での利用は防止できる。しかしながら、他の地域で使用すべきディスク（図１５（ａ）中の地域ＲＣ２用）にもコンテンツの記録が可能であり、正しくコンテンツの再生が可能である。コンテンツのディジタルコピーが可能な記録媒体では、著作権者の利益を保護するために賦課金制度などが設けられ、光ディスクの販売時に料金に上乗せされて回収されている。しかしながら、上乗せされる賦課金は国毎に異なるため、他の国で使用されるべき記録媒体が不正に利用されると、本来、利益を得るべき著作権者に正しく配分されない可能性が有る。

【００８０】また、図１５（ｂ）に示すように、地域識別子が光ディスクの出荷時に予め改ざんできない方法により記録しておくことで、他の地域で使用されるべき光ディスクへのコンテンツのコピーや再生を防止することができる。同様に、データカテゴリ識別子をディスク識別情報として記録した場合には、記録するデータが有するカテゴリ識別子と比較することで、データを記録及び再生可能なディスクへのコンテンツのコピーや再生を制限できる。光ディスク毎で固有なディスク識別子をディスク識別情報として記録した場合には、記録するデータをディスク識別子で暗号化するなどして、その光ディスクでのみ利用可能とすることができる。

【００８１】本実施形態において、ディスク識別情報によってスクランブルされるデータは、著作権保護が必要なＡＶデータやコンピュータデータでもよいし、ＡＶデータやコンピュータデータに施されているスクランブルを解くためのデスクランブルキーでもよい。

【００８２】図１３は、第１の実施形態の変形例に係る、暗号化デスクランブルキーから正規のデスクランブルキーであるか否かを判定するための方法を示すブロック図である。図１３に示すように、デスクランブルキーに、デスクランブルキーの誤りを検出するための誤り検出コードを付加したデータを、ディスク識別情報を用いてスクランブルすることにより計算した暗号化デスクランブルキーを光ディスクに記録してもよい。光ディスク再生装置では、暗号化デスクランブルキーをデスクランブルキーと誤り検出コードとに復号し、復号された誤り検出コードにおけるパリティチェックなどに基づいて誤

り検出することにより復号されたデスクランブルキーが正規のものであるか否かを判定する。例えば、異なるディスク識別情報によってデスクランブルした場合、誤ったデスクランブルキーが生成され、誤り検出コードをチェックすることにより、正規のデスクランブルキーでないことを判定できるので、不正なコピーを検出することができる。

【００８３】なお、ディスク識別情報を記録する別の方法として複数種類のディスク識別情報をプリピットで作成したスタンパを用意しそれぞれから光ディスクを作成することによって、異なるスタンパから作成される光ディスク毎で異なる利用制限を与えるようにしてもよい。さらに、ディスク識別情報を、秘密鍵を用いてスクランブルしてスクランブルされたディスク識別情報を光ディスクに記録しておくことによって、ディスク識別情報に記述される著作権の保護レベルを利用者にわからなくし、その結果、著作権保護がより強化される。

【００８４】図４において説明したキーに関する情報としてデスクランブルキーそのものを記録した場合（第１の実施形態の変形例）と、ディスク上の別領域に記録したデスクランブルキーへのポインタであるキーインデックスを記録した場合（第１の実施形態）について、図６（ａ）及び図６（ｂ）を参照して説明する。ここで、図６（ａ）は第１の実施形態の変形例に係る、図１のセクタデータ４０１にデスクランブルキー及びＡＶデータを記録する記録方法を示すブロック図であり、図６（ｂ）は第１の実施形態に係る、図１のセクタデータ４０１にデスクランブルキーへのキーインデックス及びＡＶデータを記録する記録方法を示すブロック図である。

【００８５】図６（ａ）の場合においては、同一のセクタデータ４０１に、メインデータ４０３と、メインデータ４０３をデスクランブルするために必要なキー情報４０８ａであるデスクランブルキーとを記録する。このため、ＡＶデータの記録時には、デスクランブルに必要なデスクランブルキーを取得しておく必要がある。つまり、ＡＶデータの記録時にキーそのものの入手や購入が不可欠である。

【００８６】一方、図６（ｂ）の場合では、同一のセクタデータ４０１に、メインデータ４０３と、メインデータ４０３をデスクランブルするために必要な情報を記録するデスクランブルキー領域を参照するキー情報４０８であるキーインデックスとを記録し、キーインデックスにて指定される領域にデスクランブルキーを記録する。ＡＶデータの記録時には、記録するコンテンツで使用されるキーの中のどのキーでデータがデスクランブルできるのかを示すキーＩＤを取得し、コンテンツ情報に含まれるキーインデックスリストからキーＩＤに対応するキーインデックスであるキー情報４０８を取得し、メインデータ４０３とともに記録する。デスクランブルキーの記録はデスクランブルキーを入手した際に行われ、キーＩＤに対応するキーインデックスにより示されるデスクランブルキー領域に記録される。この結果、ＡＶデータとそれに対応するデスクランブルキーの記録は独立して行うことができる。つまり、ＡＶデータの記録とキーの入手又は購入は独立に行うことができ、ＡＶデータの記録時にキーの入手又は購入は必ずしも必要でなくなる。利用者はコンテンツを記録しておいて、実際に再生する際にキーを入手するという利用法が可能となる。

【００８７】図１４は、第１の実施形態の変形例に係る、デスクランブル領域管理テーブルの構成を示す図である。以上の実施形態においては、暗号化されたコンテンツとその暗号を解くためのデスクランブルキーを関連付けるために、同一セクタデータ４０１にデスクランブルキーを参照するためのキーインデックスを記録する場合について説明したが、暗号化されたコンテンツが記録されるセクタのアドレス範囲とデスクランブルキーとの対応関係を管理する図１４のデスクランブル領域管理テーブルを用いてもよい。このデスクランブル領域管理テーブルでは、暗号化されたコンテンツが記録されるセクタのアドレス範囲が開始アドレスと終了アドレスで表され、それらのセクタのデータを再生する場合に、デスクランブルキーを参照し、暗号化されたコンテンツをデスクランブルする。

【００８８】記録するコンテンツと、そこで使用されるデスクランブルキーを取得するために、コンテンツを識別可能とするコンテンツＩＤを利用する。図５に示したように光ディスク上に記録したコンテンツ情報領域５０２内のコンテンツ管理リストに記録されるコンテンツ情報中に、コンテンツＩＤとそのコンテンツで使用されるデスクランブルキーのリストとして記録される。１つのコンテンツに対して複数のデスクランブルキーを使用できるようなリスト構成を取ることによって、一部のコンテンツやソフトウェアの切り売りするようなサービスが可能となる。

【００８９】また、図１３を参照して上述した変形例においては、チェックサムや巡回冗長検査符号などのエラー検出コードが付加されたデスクランブルキーをディスク識別情報でスクランブルしたデータを他のディスクへ不正にコピーした場合には、異なるディスク識別情報でデスクランブルを行うことによりエラーとして検出される。このような場合に、このデスクランブルキーを光ディスク上に記録されているディスク識別情報によってスクランブルされたデスクランブルキーを入手し、それに置きかえることによって正しく再生できるようなディスクを作成することもできる。

【００９０】図１のキー管理情報領域１０７は書き換え可能なリードイン領域１０１に記録される。通常、ユーザデータ領域１０２はパーソナルコンピュータのドライブ装置からアクセス可能なユーザ領域と、光ディスク上の欠陥セクタに対するスペア領域とからなり、通常の読

み出しコマンドや書き込みコマンドでは、ユーザ領域のみが論理的な連続領域としてアクセス可能である。キー管理情報をリードイン領域１０１に配置することにより、パーソナルコンピュータのドライブ装置などから直接アクセスされることを防止し、パーソナルコンピュータからＡＶデータ等に施されたスクランブルを解くためのキーの取得を不可能とすることができる。

【００９１】＜第２の実施形態＞図７は、本発明に係る第２の実施形態である光ディスク記録再生装置の構成を示すブロック図である。この光ディスク記録再生装置は、第１の実施形態に係る光ディスク１００に著作権保護を必要とする画像データや音楽データなどのＡＶデータのコンテンツを記録する装置である。

【００９２】図７において、７０１は第１の実施形態の光ディスク、７０２は半導体レーザと光学素子から構成される光ピックアップである光ヘッド、７０３は半導体レーザの動作制御及び再生信号の２値化を行う記録再生制御回路、７０４は記録すべきディジタルデータをディジタル変調するとともに２値化された再生信号をディジタル復調する変復調回路、７０５は光ディスク７０１上の傷や埃等で生起したエラーの誤り検出及び訂正処理と、誤り検出及び訂正処理に必要な誤り訂正コードの生成処理を行う誤り検出及び訂正回路、７０６は誤り検出及び訂正回路７０５の作業用メモリ及びデータバッファメモリとして用いるＲＡＭであるバッファメモリ、７０７はスクランブルされて記録されているＡＶデータをデスクランブルするデスクランブル回路、７０８は圧縮されて記録された動画データ等を伸長するＭＰＥＧ復号回路、７０９は伸長された画像データをＤ／Ａ変換してビデオ信号及びオーディオ信号を生成して出力する出力回路、７１０は光ディスク記録再生装置全体の動作を制御する制御ＣＰＵ、７１１はコンテンツに施された暗号を解くデスクランブルキーを取得する通信回路、７１２はセットトップボックスなどの通信端末装置から画像データや音楽データなどの暗号化されたコンテンツのディジタルデータを受信するデータ受信回路である。

【００９３】以上のように構成された、図７の光ディスク記録再生装置におけるデータ記録動作について説明する。セットトップボックスやＭＰＥＧエンコーダなどの通信端末装置から送信されてきた画像データや音楽データなどの暗号化されたコンテンツのディジタルデータはデータ受信回路７１２によって受信された後、バッファメモリ７０６に一時的に保存される。誤り検出及び訂正回路７０５は、保存されたコンテンツのディジタルデータに、光ディスク７０１の傷や埃等に起因する誤りの検出及び訂正処理に必要な誤り検出及び訂正コードを生成し、記録データを再構成する。誤り検出及び訂正コードには、例えば公知のリードソロモン符号などの符号が用いられる。ここで、再構成された記録データは、コンテンツのディジタルデータと、誤り検出及び訂正コードとを含む。変復調回路７０４は、記録の際に８／１６変調方式などの変調方式を用いて、記録データをディジタル変調する。そして、記録再生制御回路７０３は、ディジタル変調された記録データに従って、光ヘッド７０２から出力されるレーザ光のパワーを強度変調して、当該レーザを光ディスク７０１に照射することにより、記録データを光ディスク７０１上に記録する。

【００９４】図８は、図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるＡＶデータの記録処理を示すフローチャートである。

【００９５】図８において、まず、ステップＳ８０１において、光ディスク７０１からのＡＶデータの記録に先立ち、リードイン領域１０１のディスク識別情報を再生し、次いで、ステップＳ８０２において、ディスク識別情報に記録されている、ユーザデータ領域１０２に記録可能なデータの種別から、現在記録しようとしているコンテンツのディジタルデータが記録可能であるか否かを判断する。ステップＳ８０２でＹＥＳのときはステップＳ８０３に進む一方、ＮＯであるときはステップＳ８１０で記録動作を中止して当該ＡＶデータの記録処理を終了する。

【００９６】ステップＳ８０３では、リードイン領域１０１においてキー管理情報が記録されたセクタのデータを再生し、ステップＳ８０４では、再生したキー管理情報にコンテンツの記録に必要なキー情報に対する領域が割り当て済みであるか否かを判断する。ステップＳ８０４でＮＯであるときは、キー管理情報領域１０７にキー情報を記録するための領域を割り当てた後、ステップＳ８０６に進む。一方、ステップＳ８０４でＹＥＳのときはそのままステップＳ８０６に進む。

【００９７】コンテンツの記録を行う場合には、光ディスク記録再生装置の制御ＣＰＵ７１０は、記録する暗号化されたコンテンツのデータと、暗号を解くためのデスクランブルキーに関する情報を、通信端末装置からデータ受信回路７１２を介して受信する。ここで、キーに関する情報とは、コンテンツで使用されるキーそのもの、もしくは、コンテンツ全体で使用するキーのうち何番目のキーに対応するのかを示すキーＩＤである。キーＩＤを受信した場合に、ステップＳ８０６では、受信されたキーＩＤを、キーＩＤに対応するデスクランブルキーが記録されている領域を示すポインタであるキーインデックスに変換し、変換されたデスクランブルキーを、そのデスクランブルキーで復号されるコンテンツのデータが記録されるセクタのヘッダ領域に配置される。そして、ステップＳ８０７では、制御ＣＰＵ７１０は、記録再生制御回路７０３と、変復調回路７０４と、誤り検出及び訂正回路７０５とを制御することにより、以下の記録データの処理を実行する。この処理では、記録したいセクタデータに対してエラー検出及び訂正用のコードを付加し、これらのコードが付加されたセクタデータを、公知

の８／１６変調方式などの変調方式を用いてディジタル変調し、所定の記録位置に光ヘッド７０２を制御するとともに、ディジタル変調された記録データに従ってレーザ光を強度変調する。これによって、記録データを光ディスク７０１上に記録する。さらに、ステップＳ８０８では、コンテンツの記録の終了であるか否かを判断し、ＮＯであるときはステップＳ８０６に戻り、上記の処理を繰り返す。ステップＳ８０８でＹＥＳであれば、ステップＳ８０９で、更新されたキー管理情報を光ディスク７０１上のキー管理情報領域１０７に記録して当該ＡＶデータの記録処理を終了する。

【００９８】図９は、図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるキー管理情報領域の割り当て処理を示すフローチャートである。この処理は、コンテンツのデータの記録に先立ち、デスクランブルキーを記録するための領域を割り当てる処理である。

【００９９】図９において、まず、ステップＳ９０１において、例えば電子プログラムガイド等から記録するコンテンツのキーに関する情報（使用するデスクランブルキーの個数などを含む。）を取得し、次いで、ステップＳ９０２では、光ディスク７０１に記録されているキー管理情報領域１０７内のキー管理情報を再生し、ステップＳ９０３において、デスクランブルキー領域５０５の空き領域をキーステータス領域５０６から調べ、記録しようとしているコンテンツで使用するデスクランブルキーを記録できるか否かを判定する。ステップＳ９０３でＮＯであるときは、ステップＳ９０７で記録動作を中止して当該割り当て処理を終了する。一方、ステップＳ９０３でＹＥＳであるときは、ステップＳ９０４で、記録するコンテンツをコンテンツ情報領域５０２内のコンテンツリストに登録し、ステップＳ９０５においてデスクランブルキー領域５０５に対して、デスクランブルキーの記録に必要な領域を予約するために、対応するキーステータス領域に領域予約済みフラグを設定することにより記録用領域を割り当てる。さらに、ステップＳ９０６で、デスクランブルキーを記録するために割り当てられた領域を示すキーインデックスをキーリストとして作成し、コンテンツ情報としてのポインタを割り当てた後、当該割り当て処理を終了する。

【０１００】図１０は、図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるデスクランブルキーの記録処理を示すフローチャートである。この記録処理は、キー管理センターからデスクランブルキーを取得して光ディスク７０１に記録するための処理である。

【０１０１】図１０において、まず、ステップＳ１００１において、光ディスク７０１のリードイン領域１０１のディスク識別情報を再生した後、ステップＳ１００２において、キー管理センターからデスクランブルキーを取得するために、ディスク識別情報と、所望のコンテンツのデスクランブルに必要なキーを識別するためのキーＩＤを通信回路７１１を介してキー管理センターに送信する。キー管理センターでは、与えられたキーＩＤからコンテンツのデスクランブルに必要なデスクランブル鍵を選択し、送られてきたディスク識別情報等の情報によって、デスクランブルキーを暗号化して返信する。

【０１０２】ステップＳ１００３で、キー管理センターから通信回路７１１を介して、キーＩＤに対応するデスクランブルキーを取得した後、ステップＳ１００４で、キー管理情報領域１０７のデータを再生し、再生されたキー管理情報領域１０７内のデータのうちキーＩＤで示されるキーインデックスリストから、デスクランブルキーを記録する領域を示すキーインデックスを取得する。次いで、ステップＳ１００５において、キーインデックスにより示されたデスクランブルキー領域に上記取得したデスクランブルキーを配置し、対応するキーステータス領域５０６にキー取得済みを示す取得済みフラグを設定する。さらに、ステップＳ１００６で、すべてのキーの取得が終了したか否かが判断され、ＮＯであれば、ステップＳ１００３に戻り上記の処理を繰り返す。一方、ステップＳ１００６でＹＥＳであるときは、ステップＳ１００７において、更新されたキー管理情報をキー管理情報領域１０７に記録して当該デスクランブルキーの記録処理を終了する。

【０１０３】次いで、本実施形態の光ディスク記録再生装置のデータ再生動作について図７を参照して説明する。光ディスク７０１に記録されたディジタルデータは、以下のようにして再生される。光ヘッド７０２の半導体レーザからのレーザ光は光ディスク７０１に照射され、そのときに光ディスク７０１で反射される反射光が光ヘッド７０２を介して記録再生制御回路７０３に入射する。記録再生制御回路７０３は、入射する反射光を光電変換した後、増幅及び２値化処理を実行することにより、ディジタル化された再生信号を生成して変復調回路７０４に出力する。変復調回路７０４は、記録の際に公知の８／１６変調方式などの変調方式を用いてディジタル変調された信号をディジタル信号にディジタル復調して、誤り検出及び訂正回路７０５に出力する。次いで、誤り検出及び訂正回路７０５は、バッファメモリ７０６を作業用メモリとして用いて、光ディスク７０１の傷や埃など起因する誤りの検出及び訂正処理を実行する。この誤り検出及び訂正処理は、例えば、既知のリードソロモン符号などの復号を行うことで実行される。

【０１０４】誤り検出及び訂正処理された再生データは、デスクランブル処理を行うために、デスクランブル回路７０７に出力される。デスクランブル回路７０７は、予めデータの再生に先立って再生したキー管理情報領域１０７のデスクランブルキーを用いて再生データにデスクランブル処理を施した後、ＭＰＥＧ復号回路７０８に出力する。次いで、ＭＰＥＧ復号回路７０８は、圧縮された動画データや音楽データを伸長した後、伸長後

のデータを出力回路７０９に出力する。さらに、出力回路７０９は、入力される伸長されたデータをビデオ信号及びオーディオ信号にＤ／Ａ変換して、テレビジョン装置やオーディオ機器などの上位の機器に出力する。

【０１０５】図１１は、図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるＡＶデータの再生処理を示すフローチャートである。図１１において、まず、ステップＳ１１０１において、光ディスク７０１からのＡＶデータの記録に先立ち、リードイン領域１０１内のディスク識別情報を再生し、ステップＳ１１０２において、ディスク識別情報に記録されている再生可能なデータの種別から、現在再生しようとしているコンテンツが再生可能であるか否かを判断する。ステップＳ１１０２でＮＯであるときは、ステップＳ１１１２で再生動作を中止して当該ＡＶデータの再生処理を終了する。一方、ステップＳ１１０２でＹＥＳであるときは、ステップＳ１１０３で、リードイン領域１０１のキー管理情報領域１０７内でキー管理情報が記録されたセクタのデータを再生し、ステップＳ１１０４において再生したキー管理情報において、コンテンツの再生に必要なキー情報が記録済みであるか否かを判断する。ステップＳ１１０４でＹＥＳであるときはそのままステップＳ１１０６に進む一方、ＮＯであれば、ステップＳ１１０５において、キーを管理しているキー管理センターから通信回路７１１を介してデスクランブルキーを取得し、光ディスク７０１のキー管理情報領域１０７に記録してステップＳ１１０６に進む。

【０１０６】次いで、ステップＳ１１０６では、制御ＣＰＵ７１０は、光ディスク７０１のユーザデータ領域に光ヘッド７０２を移動させ、記録再生制御回路７０３、変復調回路７０４、誤り検出及び訂正回路７０５を制御してＡＶデータを再生する。そして、ステップＳ１１０７では、再生されたセクタのヘッダに含まれるキーインデックスにより示されるデスクランブルキー領域５０５から、セクタデータのデスクランブルに必要なデスクランブルキーを取得し、ステップＳ１１０８では、デスクランブルキーに対して行われているスクランブルを、ディスク識別情報によってデスクランブルすることにより復号する。さらに、ステップＳ１１０８において、デスクランブルキーに付与されているエラー検出コードをチェックすることにより、デスクランブルキーに誤りがあるか否かを判断する。ステップＳ１１０８でＹＥＳであるときは、不正に入手したコンテンツ（又は不正にコピーしたコンテンツ）とみなし、ステップＳ１１１２で再生動作を中止して当該ＡＶデータの再生処理を終了する。

【０１０７】一方、ステップＳ１１０８でＮＯであるときは、Ｓ１１０９において、デスクランブルキーによりコンテンツのデータをデスクランブルし、ステップＳ１１１０において、デスクランブルされたＡＶデータをＭＰＥＧ復号回路７０８に出力する。そして、制御ＣＰＵ７１０は、ＭＰＥＧ復号回路７０８及び出力回路７０９を制御することにより、デスクランブルされたＡＶデータをＭＰＥＧ伸長した後、ビデオ信号とオーディオ信号にＤ／Ａ変換してテレビジョン装置やオーディオ機器などの上位機器に出力する。次いで、ステップＳ１１１１では、コンテンツの再生の終了か否かが判断され、ＮＯであるときはステップＳ１１０６に戻り、上記の処理を繰り返す。一方、ステップＳ１１１１でＹＥＳのときは当該ＡＶデータの再生処理を終了する。

【０１０８】なお、ステップＳ１１０９で誤りが検出された場合には、不正に入手したコンテンツとみなし、例えば、不正にコピーしたコンテンツとみなし、再生動作を中止したが、キーが記録されていない場合と同様に、ステップＳ１１０５の処理を実行することにより、通信回路７１１を介して、キーを管理しているキー管理センターからキー情報を取得し、光ディスク７０１のキー管理情報領域１０７に記録してもよい。これにより、コピーしたＡＶデータであっても、キーを正規に入手することによって再生可能にすることができる。

【０１０９】図１２は、図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるデスクランブルキーの取得処理を示すフローチャートである。この処理は、再生されたキーインデックスからデスクランブルキーを再生する処理であり、図１１に図示されたＡＶデータの再生処理に先立って実行される。

【０１１０】図１２において、まず、ステップＳ１２０１では、再生されたセクタ領域のデータがスクランブルされているか否かをスクランブル制御情報により判断し、ＮＯであるときはステップＳ１２０６に進む一方、ＹＥＳであるときは、ステップＳ１２０２において上記セクタ領域と同一のセクタ領域内に記録されているキー情報を再生することによりキーインデックスを取得し、次いで、ステップＳ１２０３においてデスクランブルキー領域５０５から上記キーインデックスによって示されるデスクランブルキーを取得した後、ステップＳ１２０４では、取得されたデスクランブルキーをディスク識別情報を用いてデスクランブルし、エラー検出コードを調べることによりデスクランブルキーが誤りがあるか否かを判断する。ステップＳ１２０４でＹＥＳのときは、ステップＳ１２０５で再生動作を中止して当該デスクランブルキーの取得処理を終了する。一方、ステップＳ１２０４でＮＯであるときは、ステップＳ１２０６に進む。再生されたセクタがスクランブルされていない場合やデスクランブルキーをディスク識別情報によってデスクランブルされた結果に誤りがない場合には、ステップＳ１２０６において再生動作の許可を行い、再生されたセクタのデータを出力して当該デスクランブルキーの取得処理を終了する。

【０１１１】以上説明したように、本発明に係る実施形

態の光ディスク及び光ディスク記録再生装置では、ディスク製造段階で作成された再生専用のディスク識別情報を用いて利用者による記録や再生動作を制御するできる。さらに、上記のディスク識別情報を用いてデータの一部をスクランブルすることにより、ユーザデータ領域の物理コピーが行われたディスクに対して正常に再生すること防止することができる。また、データのデスクランブルに必要なデスクランブルキーをデータとは別領域に配置することにより、コンテンツの記録とデスクランブルキーの記録を独立に行うことができる。このため、コンテンツを記録しておき、必要に応じて、例えばコンテンツのデータの再生時に、デスクランブルキーを取得することにより、コンテンツの再生可能な状態とすることができる。この際、デスクランブルキーをディスク識別情報によりスクランブルしておくことで、上述した場合と同様に、物理的なコピーによる不正な利用を防止できることは明らかである。それに加えて、不正にコピーしたディスクであっても、その光ディスクのディスク識別情報でスクランブルされたデスクランブルキーを正式にキー管理センターから取得し、光ディスクに記録することにより、正しく再生できる光ディスクにすることもできる。

【０１１２】なお、光ディスク記録再生装置に入力されるコンテンツのデータについて既に暗号化されたものについて説明したが、光ディスク記録再生装置内にコンテンツを暗号化する回路を備えることで、入力されたコンテンツのデータを暗号化し、光ディスク上に記録することにより同様の効果が得られる。

【０１１３】また、本実施形態では、暗号化されたコンテンツの解読に必要なデスクランブルキーのみをディスク識別情報を用いて暗号化することにより、異なるディスク識別情報を有するディスク間でのコピーの防止を行ったが、コンテンツ自身にディスク識別情報を用いた暗号化を施すことにより、同様にコピーの防止を行うことができる。さらに、ディスク識別情報にも秘密鍵を用いて暗号化を施すことにより、ディスク上に記録されたコンテンツの不正な解読をより困難にすることができる。

【０１１４】＜第１及び第２の実施形態の効果＞本発明に係る実施形態の光ディスクは、ユーザデータ領域への記録動作や再生動作を光ディスク毎に行うディスク識別情報が書き換え不可能な再生専用領域に記録されることにより、利用者による光ディスク上へのコンテンツの記録動作や再生動作を光ディスクの製造時に記録する情報を用いて制御することができる。

【０１１５】本発明に係る実施形態の光ディスクは、書き換えが不可能な再生専用のディスク識別情報を鍵として暗号化されたデータが光ディスク上のユーザデータ領域に記録することにより、利用者によるユーザデータ領域の他の記録型光ディスクにコピーしたとしても、ディスク識別情報をコピーすることができず、データの正しい復号並びに再生が不可能とすることができる。

【０１１６】本発明に係る実施形態の光ディスクは、暗号化されたデータと暗号を解くデスクランブルキーとが異なるセクタ領域に記録されることにより、映画や音楽などの著作権保護が必要なデータの取得と暗号を解くためのデスクランブルキーの取得を独立に行うことが可能となる。さらに、ディスク識別情報を鍵としてデスクランブルキーを暗号化して記録することにより、利用者によるユーザデータ領域の他の記録型光ディスクにコピーしたとしても、ディスク識別情報をコピーすることができず、データの正しい復号並びに再生が不可能とし、コピー先の光ディスクのディスク識別情報を鍵として暗号化したデスクランブルキーを取得し記録することで、データの正しい復号並びに再生を可能とすることができる。

【０１１７】＜第３の実施形態＞次いで、本発明に係る第３の実施形態である暗号化コンテンツ記録及び再生方法について図面を参照しながら説明する。図１６は、本発明に係る第３の実施形態である光ディスク１１０１のデータ記録領域を示す平面図である。

【０１１８】図１６において、１１０１はディジタルデータを記録することが可能な記録媒体であって、書き換え型又は追記型の光ディスクである記録型光ディスク、１１０２はディスク情報が微小な凹凸ピットの形式で記録されたコントロールユーザデータ領域、１１０３はレーザ光の光ビームを光ディスクに照射することによりユーザがデータを記録するユーザデータ領域、１１０４はディスクＩＤが記録されたＢＣＡである。ＢＣＡ１１０４において、コントロールユーザデータ領域１１０２の内周部分の微小な凹凸ピット上の記録膜は、半径方向に長い形状でかつ複数個のトリミング領域１１０５が形成されるように、その記録膜に対して部分的にＹＡＧレーザなどのパルスレーザのレーザ光を放射することによりトリミングされ、これによりデスクランブル識別情報であるディスクＩＤが記録される。

【０１１９】図１７は、第３の実施形態に係るＢＣＡ再生回路１４０１における再生信号１２０１及び再生２値化信号１２０７の信号波形を示す波形図であり、図１８は、第３の実施形態に係るＢＣＡ再生回路１４０１の構成を示すブロック図である。図１７において、ＢＣＡ１１０４のデータを再生したときの再生信号１２０１を示している。図１８において、１３０１は光ピックアップ、１３０２はプリアンプ、１３０３は低域通過フィルタ（ＬＰＦ）、１３０４は２値化回路、１３０５は復調回路である。

【０１２０】図１８において、光ピックアップ１３０１から出力されるレーザ光は光ディスク１１０１のＢＣＡ１１０４を照射し、その反射光は光ピックアップ１３０１により光電変換された後、光電変換後の電気信号は、プリアンプ１３０２で増幅されて再生信号１２０１が得

られる。ここで、図１７の再生信号１２０１はコントロールユーザデータ領域１１０２の凹凸ピットに応じたレベルを有する信号であり、この再生信号１２０１において、１２０２、１２０３、１２０４はパルスレーザによるトリミング処理により記録膜が取り除かれて、凹凸ピットによる信号が欠落しているトリミング部分である。このトリミング処理は、光ディスクの製造者によって行われる。

【０１２１】図１８に戻り説明すると、再生信号１２０１は低域通過フィルタ１３０３に入力されて、凹凸ピットによる変調信号が除去された後に、２値化回路１３０４に入力される。２値化回路１３０４に入力された再生信号は、コントロールユーザデータ領域１１０２の信号を２値化する通常のスライスレベル１２０５ではなく、スライスレベル１２０５よりも十分に低いレベルであるスライスレベル１２０６を用いて２値化されて、再生２値化信号１２０７が得られる。２値化回路１３０４から出力される再生２値化信号１２０７は、復調回路１３０５で復調されてディスクＩＤ信号１３０６が得られる。

【０１２２】以上説明したように、光ディスクを識別するディスク識別情報を付加することにより、光ディスクの管理を容易に実現することができる。また、ＢＣＡ１１０４が凹凸ピット上に記録されることにより、ＢＣＡ１１０４内の光ディスクを識別する情報が容易に改ざんされることを防止することができる。さらに、図１６のコントロールユーザデータ領域１１０２とＢＣＡ１１０４が隣接していることにより、コントロールユーザデータ領域１１０２のデータを再生する際に、ＢＣＡ１１０４のデータも続けて再生することができ、もしくはＢＣＡ１１０４のデータを再生する際に、コントロールユーザデータ領域１１０２のデータを続けて再生することができるので、例えば光ディスクを起動する際にＣＰＵが速やかに光ディスクを識別するためのＢＣＡ１１０４の情報を入手し、暗号化されたコンテンツを記録するための処理を早めることが可能になる。

【０１２３】なお、本実施形態のＢＣＡ１１０４は、コントロールユーザデータ領域１１０２の内周部分の凹凸ピット上の記録膜をトリミングすることにより形成されているが、書き換え型又は追記型の光ディスクである記録形光ディスクを構成する記録膜は、再生専用の光ディスクにおける反射膜に対して熱による影響を受けやすい。コントロールユーザデータ領域１１０２の内周部分をトリミングすることにより、外周部分をトリミングする場合に比べて、トリミングの際に発生する熱からユーザデータ領域１１０３を保護することができる。また、コントロールユーザデータ領域１１０２の内周側にＢＣＡ１１０４を形成するのは、フォーカスサーボ回路の不安定性によりレーザ光のビームのスポットの径が変化する場合のマージンを考慮しているためである。

【０１２４】なお、トリミング前のＢＣＡ１１０４に記録されているデータが、コントロールユーザデータ領域１１０２に記録されていてもよい。ＢＣＡ１１０４に記録されているデータが、コントロールユーザデータ領域１１０２にも記録されていることにより、トリミングを行ってもコントロールユーザデータ領域１１０２の上記データを保護することができる。さらに、ＢＣＡ１１０４に記録されているデータが、ＢＣＡ１１０４から、コントロールユーザデータ領域１１０２まで連続して繰り返し記録されている場合には、コントロールユーザデータ領域１１０２の上記データを見つけることによって、ＢＣＡ１１０４の位置を予想することができる。

【０１２５】次いで、上記ＢＣＡ１１０４を有する光ディスク１１０１に、ネットワークを介して、ディスクＩＤで暗号化されたコンテンツを記録する手順を述べる。第３乃至第５の実施形態において、ネットワークとは、例えば、インターネット、公衆電話回線、又は専用線などの通信網をいう。図１９は、第３の実施形態に係る光ディスク記録再生システムの構成を示すブロック図であり、上記ＢＣＡ１１０４を有する書き換え型又は追記型の光ディスクである記録型光ディスク１１０１に暗号化コンテンツを記録する装置構成を示す。

【０１２６】図１９において、光ディスク記録再生システムは、互いにインターネットなどのネットワーク１４０５を介して接続された、光ディスク記録再生装置１４１０と、暗号化部１４０６とを備えて構成される。光ディスク記録再生装置１４１０は、光ピックアップ１３０１と、ＢＣＡ再生回路１４０１と、インターネット４０３と、記録回路１４１１と、データ再生部１４１２と、暗号デコーダ１４１３とを備える。また、暗号化部１４０６は、インターフェース１４０４と、コンテンツメモリ１４０７と、暗号化エンコーダ１４０８とを備える。

【０１２７】まず、光ピックアップ１３０１から出力されるレーザ光は、例えばＲＡＭ型光ディスク１１０１のＢＣＡ１１０４を照射し、その反射光は光ピックアップ１３０１によって光電変換された後、光電変換された再生信号がＢＣＡ再生回路１４０１に入力される。ＢＣＡ再生回路１４０１は入力された再生信号に基づいてＢＣＡ内のディスクＩＤ信号１４０２を再生して、再生されたディスクＩＤ信号１４０２を暗号デコーダ１４１３に出力するとともに、インターフェース１４０３及び１４０４とネットワーク１４０５を介して、暗号化部１４０６の暗号化エンコーダ１４０８に送られる。暗号化エンコーダ１４０８は、コンテンツメモリ１４０７内のコンテンツのデータが記録される光ディスク１１０１のディスクＩＤ信号１４０２が暗号を解く復号鍵となるように、当該コンテンツのデータを暗号化し、又は画像音声用のスクランブルを行う。

【０１２８】なお、本実施形態では、暗号化処理について、コンテンツ１４０７を、ディスクＩＤ信号１４０２を暗号鍵として用いて暗号化すると表現しても同一の意

味とする。また、本実施形態においては、暗号化や復号化を、錠と鍵の関係で考え、上記錠を上記鍵で閉めることを暗号化とし、上記錠を上記鍵で開けることを復号化とする。従って、暗号化と復号化で実際の演算は異なるが、暗号化するための鍵と復号化するための鍵は、同一であるとする。なお、コンテンツ１４０７をＣとし、ディスクＩＤ信号１４０２をＢＣＡＳとし、暗号化されたコンテンツ１４０９をＣ［ＢＣＡＳ］とし、暗号化処理の演算を＊で表し、次式のように表記する。

【０１２９】

【数１】Ｃ＊ＢＣＡＳ＝Ｃ［ＢＣＡＳ］

【０１３０】暗号化部１４０６によって暗号化されたコンテンツ１４０９は、インターフェース１４０３及び１４０４とネットワーク１４０５を介して記録再生装置１４１０の記録回路１４１１に送られる。記録回路１４１１は、入力されるコンテンツのデータを所定のディジタル変調し、ディジタル変調されたデータに応じて光ピックアップ１３０１からのレーザ光を強度変調して光ディスク１１０１に照射することにより、コンテンツのデータを光ディスク１１０１に記録する。

【０１３１】次に、光ディスク１１０１に暗号化されて記録された上記コンテンツを再生する際は、光ピックアップ１３０１から出力されるレーザ光がユーザデータ領域１１０３の上記暗号化コンテンツが記録された領域を照射し、その反射光が光ピックアップ１３０１によって光電変換された後、光電変換された再生信号がデータ再生部１４１２に入力される。データ再生部１４１２は、入力された再生信号をディジタルデータにＡ／Ｄ変換して暗号デコーダ１４１３に出力する。一方、光ピックアップ１３０１からのレーザ光は光ディスク１１０１のＢＣＡ１１０４を照射し、その反射光は光ピックアップ１３０１によって光電変換された後、光電変換された再生信号はＢＣＡ再生回路１４０１に入力される。ＢＣＡ再生回路１４０１は入力された再生信号をＡ／Ｄ変換してディスクＩＤ信号１４０２を発生して、当該ディスクＩＤ信号を暗号デコーダ１４１３に出力する。

【０１３２】暗号デコーダ１４１３は、入力されたディスクＩＤ信号１４０２を鍵として用いて、暗号化されたコンテンツのデータを復号する。このとき、コンテンツが正規に光ディスク１１０１に記録されている場合は、光ディスク１１０１に記録されている暗号化コンテンツを復号するための鍵は、光ディスク１１０１のディスクＩＤ信号１４０２であり、再生時にＢＣＡ再生回路１４０１から出力されるディスクＩＤ信号１４０２も、光ディスク１１０１のディスクＩＤ信号（ＢＣＡＳ）である。従って、復号又はデスクランブルされたコンテンツが暗号デコーダ１４１３から出力信号１４１４として出力される。なお、復号化処理の演算を＃とすると、次式のように表記される。

【０１３３】

【数２】Ｃ［ＢＣＡＳ］＃ＢＣＡＳ＝Ｃ

【０１３４】ここで、コンテンツのデータが画像データの場合は、例えばＭＰＥＧ信号のデータが伸長されて、画像信号のデータが得られる。

【０１３５】以上説明したように、本実施形態における暗号化は、ディスクＩＤを鍵としており、ディスクＩＤは、１枚の光ディスクに対応して１個しか存在しないため、当該１枚の光ディスクにしか同一の暗号化コンテンツの記録をすることができないという効果がある。すなわち、上記コンテンツ１４０７を、例えばＩＤ１というディスクＩＤを持つ正規の光ディスクから、ＩＤ２という別のディスクＩＤを持つ別の光ディスクにコピーして再生しようとした場合、ＢＣＡ再生回路４０１からディスクＩＤ信号１４０２としてＩＤ２が出力される。しかしながら、暗号化コンテンツはＩＤ１というディスクＩＤ信号で暗号化されているので、暗号デコーダ１４１３で、暗号化コンテンツを復号することができない。

【０１３６】なお、暗号化エンコーダ１４０８はコンテンツの供給元ではなく、ネットワークに対して記録再生装置側にあり、暗号化エンコーダを搭載したＩＣカードなどの形態であってもよい。また、上記光ディスク１１０１はディスクＩＤのみで暗号化されているので、ＢＣＡ再生回路１４０１と暗号デコーダ１４１３を有する任意の光ディスク記録再生装置で再生することが可能である。

【０１３７】＜第４の実施形態＞次いで、本発明に係る第４の実施形態である暗号化コンテンツ記録方法について図面を参照しながら説明する。図２０は、本発明に係る第４の実施形態である光ディスク記録再生システムの構成を示すブロック図であり、ＢＣＡを有する書き換え型又は追記型光ディスクである記録型光ディスクに、暗号化コンテンツを記録する装置構成を示す。なお、第４の実施形態の説明において、第３の実施形態と共通の部分はその説明を簡略化する。

【０１３８】図２０において、第４の実施形態に係る光ディスク記録再生システムは、ＣＡＴＶ会社装置１５０１と、鍵発行センター装置１５０７と、ＣＡＴＶデコーダ１５０６と、光ディスク記録再生装置１５１４と、テレビジョン装置１５３０とを備えて構成される。ここで、ＣＡＴＶ会社装置１５０１は、映画ソフトウエアなどのコンテンツのデータを格納するコンテンツメモリ１５０２と、第１暗号鍵を格納する第１暗号鍵メモリ１５０３と、第１暗号化エンコーダ１５０４とを備える。また、鍵発行センター装置１５０７は、その装置１５０７の動作を制御する制御部１５０７ａと、時間制限情報を格納する時間制限情報メモリ１５１０と、記録許可コードを格納する記録許可コードメモリ１５１１とを備える。さらに、ＣＡＴＶデコーダ１５０６は、ＣＡＴＶデコーダ１５０６のシステムＩＤを格納するシステムＩＤメモリ１５０８と、第１暗号デコーダ１５１３と、第２

暗号化エンコーダ１５１６と、ＩＣカード１５２２内の会社識別信号メモリ１５２３とを備える。またさらに、光ディスク記録再生装置１５１４は、記録回路１５１８と、データ再生部１５１９と、ＢＣＡ再生回路１５２１と、第２暗号デコーダ１５２０と、ＩＣカード１５２４内の会社識別信号メモリ１５２６とを備える。

【０１３９】まず、ＣＡＴＶ会社装置１５０１の第１暗号化エンコーダ１５０４は、映画ソフトウエアなどのコンテンツメモリ１５０２内のコンテンツのデータを第１暗号鍵１５０３を用いて暗号化することにより、第１暗号化コンテンツ１５０５を生成し、生成された第１暗号化コンテンツ１５０５をネットワークを介して各ユーザのＣＡＴＶデコーダ１５０６の第１暗号化デコーダ１５１３に送信する。ここで、コンテンツメモリ１５０２内のデータをＣとし、第１暗号鍵１５０３をＦＫとし、第１暗号化コンテンツ１５０５をＣ［ＦＫ］とすると、次式のように表記される。

【０１４０】

【数３】Ｃ＊ＦＫ＝Ｃ［ＦＫ］

【０１４１】ＣＡＴＶデコーダ１５０６は、システムＩＤメモリ１５０８内の当該ＣＡＴＶデコーダ１５０６のシステムＩＤと、視聴もしくはＲＡＭ型光ディスク１１０１への記録を行いたい上記コンテンツに予め付与され、例えば当該ＣＡＴＶデコーダ１５０６のキーボード（図示せず。）を用いて入力されたタイトルコード１５０９とを、ネットワークを介して鍵発行センター装置１５０７に送信する。ここで、タイトルコード１５０９はＴＶの画面に従って選択することにより入力してもよいし、直接にキーボードから入力してもよいし、リモートコントローラー等から入力してもよい。従って、タイトルコード１５０９は、ユーザが独自に入手していてもよいし、第１暗号化コンテンツ１５０５とともにＣＡＴＶデコーダ１５０６に送られてきてもよいし、番組案内などの形態で第１暗号化コンテンツ１５０５とは別の時刻に予め送られていてもよい。

【０１４２】鍵発行センター装置１５０７の制御部１５０７ａは、ＣＡＴＶデコーダ１５０６のシステムＩＤと、上記コンテンツのタイトルコード１５０９とに基づいて、時間制限情報メモリ１５１０内の時間制限情報と、記録許可コードメモリ１５１１内の記録許可コードとを参照して、これらに対応する鍵（Ｋ）１５１２を記録許可コード及び時間制限コードとともにＣＡＴＶデコーダ１５０６の第１暗号デコーダ１５１３に対して、ネットワークを介して送信する。なお、時間制限情報により、同一のコンテンツを時刻を変えて複数回放送する場合を区別することができる。ここで、第１復号鍵をＦＫとし、ＣＡＴＶデコーダ１５０６のシステムＩＤをＤＩＤとし、時間制限情報をＴＩＭＥとし、記録許可コードをＣＯＰＹとし、コンテンツのタイトルコード１５０９をＴとするとき、鍵（Ｋ）は、次式の関係を満たしている。

【０１４３】

【数４】ＦＫ＝Ｋ＊Ｔ＊ＤＩＤ＊ＴＩＭＥ＊ＣＯＰＹ

【０１４４】なお、記録許可コードメモリ１５１１内の記録許可コードは、例えばＣＡＴＶ会社装置１５０１が、放送するコンテンツが新作品か旧作品かを判断して、視聴のみ許可するのか、視聴、記録の両方を許可するのかを決定する。

【０１４５】ＣＡＴＶデコーダ１５０６の第１暗号デコーダ１５１３は、第１復号鍵（ＦＫ）と、鍵（Ｋ）１５１２と、上記コンテンツのタイトルコード１５０９と、システムＩＤと、記録許可コードと、時間制限情報とが上述の関係を満たしており、かつクロック回路１５２７から出力される現在時刻情報が当該時間制限情報の条件を満たしていれば、第１暗号化コンテンツ１５０５を復号する。ここで、上記暗号化されたコンテンツが画像信号の場合は、デスクランブルされた画像信号が第１暗号化デコーダ１５１３からテレビジョン装置１５３０に出力されて視聴できる。ここで、第１暗号化デコーダ１５１３の復号化処理は次式で表される。

【０１４６】

【数５】

Ｃ［ＦＫ］＃（Ｋ＊Ｔ＊ＤＩＤ＊ＴＩＭＥ＊ＣＯＰＹ）

＝Ｃ［ＦＫ］＃ＦＫ

＝Ｃ

【０１４７】なお、記録許可コードが視聴のみ許可する場合は、光ディスク１１０１に記録できないが、視聴と記録の両方を許可する場合は記録することができるので、以下でこの方法について説明する。

【０１４８】光ディスク記録再生装置１５１４のＢＣＡ再生回路１５２１は、光ディスク１１０１のＢＣＡ１１０４のデータを再生してディスクＩＤ信号１５１５を得て、当該ディスクＩＤ信号をＣＡＴＶデコーダ１５０６の第２暗号化エンコーダ１５１６に出力する。ＣＡＴＶデコーダ１５０６の第２暗号化エンコーダ１５１６は、ディスクＩＤ信号１５１５を第２暗号鍵として用いて、第１暗号デコーダ１５１３から出力されたコンテンツのデータを暗号化することにより、第２暗号化コンテンツ１５１７を生成して光ディスク記録再生装置１５１４の記録回路１５１８に送信する。なお、第２暗号デコーダ１５１６の上記暗号化は、第１暗号デコーダ１５１３から第１暗号化コンテンツが復号されて出力されている時間に限られる。ここで、第１暗号デコーダ１５１３の出力信号であるコンテンツをＣとし、第２暗号鍵であるディスクＩＤ信号１５１５をＢＣＡＳとし、第２暗号化コンテンツ１５１７をＣ［ＢＣＡＳ］とすると、次式のように表記される。

【０１４９】

【数６】Ｃ＊ＢＣＡＳ＝Ｃ［ＢＣＡＳ］

【０１５０】光ディスク記録再生装置１５１４の記録回

路１５１８に送られた第２暗号化コンテンツ１５１７は、記録回路１５１８により、例えば公知の８／１６変調方式により変調されて、光ピックアップ（図示せず。）により光ディスク１１０１のユーザデータ領域１１０３に記録される。光ディスク１１０１に暗号化されて記録された上記コンテンツを再生する際は、光ピックアップから出力されるレーザ光が光ディスク１１０１の上記暗号化されたコンテンツが記録されている領域を照射し、その反射光が光ピックアップに入射する。上記光ピックアップは入射する反射光を光電変換し、光電変換された再生信号をデータ再生部１５１９に出力し、データ再生部１５１９は、入力された再生信号をディジタル再生信号にＡ／Ｄ変換して第２暗号デコーダ１５２０に出力する。

【０１５１】一方、光ピックアップから出力されるレーザ光は光ディスク１１０１のＢＣＡ１１０４を照射し、その反射光が光ピックアップに入射する。上記光ピックアップは入射する反射光を光電変換し、光電変換された再生信号をＢＣＡ再生回路１５２１に出力する。ＢＣＡ再生回路１５２１は入力された再生信号に基づいてディスクＩＤ信号１５１５を生成して第２暗号デコーダ１５２０に出力する。これに応答して、第２暗号デコーダ１５２０は、入力されたディスクＩＤ信号１５１５を鍵として用いて、データ再生部１５１９から出力される再生された暗号化コンテンツの復号を行う。このとき、コンテンツが正規に光ディスク１１０１に記録されている場合は、光ディスク１１０１に記録されている暗号化コンテンツを復号するための鍵は光ディスク１１０１のディスクＩＤであり、ＢＣＡ再生回路１５２１から出力されるディスクＩＤ信号も、光ディスク１１０１のディスクＩＤ信号（ＢＣＡＳ）であるので、第２暗号デコーダ１５２０は正常に復号処理を実行することができる。従って、復号又はデスクランブルされたコンテンツのデータは第２暗号デコーダ１５２０から出力信号１５２５として出力される。ここで、第２暗号デコーダ１５２０の復号化処理は次式で表記することができ、コンテンツが画像信号の場合は、第２暗号デコーダ１５２０は、例えばＭＰＥＧ信号を伸長して元の画像信号を再生して出力する。

【０１５２】

【数７】Ｃ［ＢＣＡＳ］＃ＢＣＡＳ＝Ｃ

【０１５３】また、上記光ディスク１１０１はディスクＩＤ信号（ＢＣＡＳ）１５１５のみで暗号化されているので、ＢＣＡ再生回路１５２１と第２暗号デコーダ１５２０を有する任意の光ディスク記録再生装置で再生することが可能である。なお、暗号エンコーダ１５０４，１５１６で暗号化し、暗号デコーダ１５１３，１５２０で復号化することを説明したが、各装置１５０１，１５０６，１５１４内の制御部であるＣＰＵで実行されるプログラムに、暗号アルゴリズム及び復号アルゴリズムのプログラムを備えて暗号化や復号化を実行するように構成してもよい。

【０１５４】なお、本実施形態において、ＣＡＴＶデコーダ１５０６の第２暗号化エンコーダ１５１６はディスクＩＤ信号１５１５を第２暗号鍵として用いてコンテンツを暗号化したが、以下のようにコンテンツを暗号化してもよい。例えば各ＣＡＴＶ会社装置１５０１毎に準備されたＩＣカード１５２２をＣＡＴＶデコーダ１５０６に装着して、ＩＣカード１５２２の会社識別信号メモリ１５２３内に記録されている会社識別信号と、ＢＣＡ再生回路１５２１により再生されたディスクＩＤ信号（ＢＣＡＳ）を組み合わせて第２暗号鍵として用いて、第２暗号化エンコーダ１５１６によりコンテンツを暗号化してもよい。ここで、第１暗号デコーダ１５１３の出力信号であるコンテンツをＣとし、第１の第２暗号鍵であるディスクＩＤ信号１５１５をＢＣＡＳとし、第２の第２暗号鍵である会社識別信号１５２３をＣＫとし、第２暗号化コンテンツ１５１７をＣ［ＢＣＡＳ，ＣＫ］とするとき、第２暗号化エンコーダ１５１６の暗号化処理を次式のように表記される。

【０１５５】

【数８】Ｃ＊ＢＣＡＳ＊ＣＫ＝Ｃ［ＢＣＡＳ，ＣＫ］

【０１５６】次に、光ディスク１１０１に暗号化して記録されたコンテンツを再生する際には、光ピックアップから出力されるレーザ光が光ディスク１１０１の上記暗号化されたコンテンツが記録されている領域を照射し、その反射光が光ピックアップに入射する。光ピックアップは入射される反射光を再生信号に光電変換してデータ再生部１５１９に出力する。データ再生部１５１９は入力される再生信号をディジタル再生信号にＡ／Ｄ変換して第２暗号デコーダ１５２０に出力する。一方、光ピックアップから出力されるレーザ光は光ディスク１１０１のＢＣＡ１１０４を照射し、その反射光が光ピックアップに入射する。光ピックアップは入射される反射光を再生信号に光電変換してＢＣＡ再生回路１５２１に出力する。ＢＣＡ再生回路１５２１は入力される再生信号に基づいてディスクＩＤ信号１５１５を再生して、ディスクＩＤ信号１５１５を第２暗号化エンコーダ１５１６及び第２暗号デコーダ１５２０に出力する。

【０１５７】さらに、光ディスク記録再生装置１５１４に装着されたＩＣカード１５２４の会社識別信号メモリ１５２６内の会社識別信号は、第２暗号デコーダ１５２０に入力される。なお、当該会社識別信号は、ＩＣカード１５２４の会社識別信号メモリ１５２６内に記録されていなくてもよく、例えば、光ディスク記録再生装置１５１４の記録プログラムのインストール時に、会社識別信号が、光ディスク記録再生装置１５１４の制御部であるＣＰＵに接続されたメモリ（図示せず。）に記録されていてもよい。とって代わって、会社識別信号を光ディスク記録再生装置１５１４のキーボード（図示せず。）

を用いて入力してもよい。

【０１５８】第２暗号デコーダ１５２０は、入力されたディスクＩＤ信号１５１５と、会社識別信号を復号鍵として用いて、暗号化されたコンテンツの復号を行う。このとき、ＣＡＴＶデコーダ１５０６のユーザがＣＡＴＶ会社装置１５０２を有する特定のＣＡＴＶ会社と正式に契約をし、コンテンツ１５０２が正規に光ディスク１１０１に記録されている場合は、光ディスク１１０１に暗号化されて記録されている暗号化コンテンツの第１の復号鍵は、まさに再生しようとする光ディスク１１０１のディスクＩＤ信号（ＢＣＡＳ）であり、第２の復号鍵は、契約したＣＡＴＶ会社から提供されたＩＣカード１５２４の会社識別信号メモリ１５２６内の会社識別信号（ＣＫ）である。従って、復号又はデスクランブルされたコンテンツの出力信号１５２５が、第２暗号デコーダ１５２０から出力される。ここで、第２暗号デコーダ１５２０の復号化処理は次式のように表記され、コンテンツが画像信号の場合は、例えばＭＰＥＧ信号が第２暗号デコーダ１５２０により伸長されて、画像信号の出力信号１５２５が出力される。

【０１５９】

【数９】

Ｃ［ＢＣＡＳ，ＣＫ］＃（ＢＣＡＳ＊ＣＫ）＝Ｃ

【０１６０】また、上記光ディスク１１０１のコンテンツは、ディスクＩＤ信号１５１５と会社識別信号で暗号化されているので、上記コンテンツの提供元のＣＡＴＶ会社と契約を結んでいれば、ＢＣＡ再生回路１５２１と、第２暗号デコーダ１５２０を有する任意の光ディスク記録再生装置で再生することが可能である。逆に、上記ＣＡＴＶ会社と契約していなければ、会社識別信号を入手できないので、コンテンツを再生することができず、契約済みのユーザとの差別化を可能にする。

【０１６１】また、本実施形態では、各ユーザは自宅のＣＡＴＶデコーダ１５０６に光ディスク記録再生装置１５１４からディスクＩＤ信号を送り、画像データ等を暗号化するので、ＣＡＴＶ会社装置１５０１は各ユーザに配信する暗号化コンテンツを個別に変える必要がなく、放送時のシステムを簡単にでき、低コストで、大量の視聴者に同じコンテンツを提供することができる。さらに、本実施形態によれば、ＣＡＴＶデコーダ１５０６を有する各ユーザ毎にＲＡＭ型光ディスク１枚だけに記録を許可することができる。

【０１６２】なお、本実施形態では、ケーブルテレビジョンのヘッドエンドからコンテンツを放送する場合について説明したが、電波による放送でも同様である。

【０１６３】＜第５の実施形態＞さらに、本発明に係る第５の実施形態である暗号化コンテンツ記録及び再生方法について図面を参照しながら説明する。図２１は、本発明に係る第５の実施形態である光ディスク１６０１のデータ記録領域を示す平面図であり、図２２は、第５の実施形態に係る光ディスク記録再生システムの構成を示すブロック図である。なお、第５の実施形態において、第３及び第４の実施形態と共通の部分はその説明を簡略化する。

【０１６４】図２１において、１６０１は書き換え型又は追記型光ディスクである記録型光ディスク、１６０２はディスク情報を凹凸ピットの形式で記録されたコントロールユーザデータ領域、１６０３はレーザ光の光ビームを光ディスクに照射することによりユーザがデータを記録するためのユーザデータ領域、１６０４はディスクＩＤが記録されたＢＣＡである。

【０１６５】ＢＣＡ１６０４では、コントロールユーザデータ領域１６０２の内周部分の凹凸ピット上の記録膜が部分的にＹＡＧレーザなどのパルスレーザでトリミングされることにより、半径方向に長い形状でかつ複数個のトリミング領域１６０６が形成される。なお、トリミングはディスク製造者によって行われる。また、ＢＣＡ１６０４に記録されるデータにディスクＩＤを付加することにより、光ディスクの管理を容易に実現することができる。さらに、ＢＣＡ１６０４のデータが凹凸ピット上に記録されることにより、ＢＣＡ１６０４に記録された、光ディスクを識別する情報が容易に改ざんされることを防止することができる。

【０１６６】さらに、コントロールユーザデータ領域１６０２とＢＣＡ１６０４が隣接していることにより、コントロールユーザデータ領域１６０２のデータを再生する際に、ＢＣＡ１６０４のデータも続けて再生することができ、もしくはＢＣＡ１６０４のデータを再生する際に、コントロールユーザデータ領域１６０２のデータを続けて再生することができるので、例えば光ディスクを起動する際にＣＰＵが速やかにディスクを識別するためのＢＣＡ１６０４の情報を入手し、暗号化されたコンテンツを記録するための処理を早めることが可能になる。

【０１６７】なお、本実施形態のＢＣＡ１６０４を、コントロールユーザデータ領域１６０２の内周部分の凹凸ピット上の記録膜をトリミングすることにより形成しているが、書き換え型又は追記型光ディスクである記録型光ディスクを構成する記録膜は、再生専用の光ディスクにおける反射膜に対して熱による影響を受けやすい。コントロールユーザデータ領域６０２の内周部分をトリミングすることにより、外周部分をトリミングする場合に比べて、トリミングの際に発生する熱からユーザデータ領域１６０３の記録データを保護することができる。また、コントロールユーザデータ領域１６０２の内周側にＢＣＡ１６０４を形成するのは、フォーカスサーボ回路の不安定性によりレーザ光のビームのスポットの径が変化する場合のマージンを考慮しているためである。なお、トリミング前のＢＣＡ１６０４に記録されているデータが、コントロールユーザデータ領域１６０２に記録されていてもよい。ＢＣＡ１６０４に記録されているデ

ータが、コントロールユーザデータ領域１６０２にも記録されていることにより、トリミングを行ってもコントロールユーザデータ領域１６０２の上記データを保護することができる。

【０１６８】さらに、上記データが、ＢＣＡ１６０４から、コントロールユーザデータ領域１６０２まで連続して繰り返し記録されている場合には、コントロールユーザデータ領域１６０２の上記データを見つけることによって、ＢＣＡ１６０４の位置を予想することができる。また、鍵情報記録領域１６０５のデータは、ユーザデータ領域１６０３と同じく光ビームを照射することにより記録される。

【０１６９】本実施形態のように、コントロールユーザデータ領域１６０２と鍵情報記録領域１６０５が隣接していることにより、コントロールユーザデータ領域１６０２のデータを再生する際に、鍵情報記録領域１６０５のデータも続けて再生することができ、もしくは鍵情報記録領域１６０５のデータを再生する際に、コントロールユーザデータ領域１６０２のデータを続けて再生することができるので、例えば光ディスクを起動する際にＣＰＵが速やかにディスクを識別するためのＢＣＡ１６０４の情報を入手し、暗号化されたコンテンツを再生するための処理を早めることが可能になる。

【０１７０】図２２において、第５の実施形態に係る光ディスク記録再生システムは、ＣＡＴＶ会社装置１７０１と、鍵発行センター装置１７０７と、ＣＡＴＶデコーダ１７０６と、光ディスク記録再生装置１７１４と、テレビジョン装置１７３０とを備えて構成される。ここで、ＣＡＴＶ会社装置１７０１は、映画ソフトウエアなどのコンテンツを格納するコンテンツメモリ１７０２と、第１暗号鍵を格納する第１暗号鍵メモリ１７０３と、第１暗号化エンコーダ１７０４とを備える。また、ＣＡＴＶデコーダ１７０６はシステムＩＤメモリ１７０８と、第１暗号デコーダ１７１３と、現在時刻情報を出力するクロック回路１７２５とを備える。さらに、鍵発行センター装置１７０７は、当該装置１７０７の動作を制御する制御部１７０７ａと、時間制限情報を格納する時間制限情報メモリ１７１０とを備える。またさらに、光ディスク記録再生装置１７１４は、記録回路１７１７と、鍵情報記録回路１７１９と、ＢＣＡ再生回路１７２０と、データ再生部１７２１と、第２暗号デコーダ１７２２と、鍵情報再生部１７２３とを備える。

【０１７１】まず、ＣＡＴＶ会社装置１７０１の第１暗号化エンコーダ１７０４は、コンテンツメモリ１７０２内の映画ソフトウエアなどのコンテンツのデータを第１暗号鍵１７０３を用いて暗号化することにより、第１暗号化コンテンツ１７０５を生成し、ネットワークを介して各ユーザのＣＡＴＶデコーダ１７０６の第１暗号デコーダ１７１３に送信する。ここで、コンテンツメモリ１７０２内のコンテンツをＣとし、第１暗号鍵メモリ１７０３内の第１暗号鍵をＦＫとし、第１暗号化コンテンツ１７０５をＣ［ＦＫ］とすると、次式のように表記される。

【０１７２】

【数１０】Ｃ＊ＦＫ＝Ｃ［ＦＫ］

【０１７３】ＣＡＴＶデコーダ１７０６は、ＣＡＴＶデコーダ１７０６のシステムＩＤメモリ１７０８内のシステムＩＤと、例えばキーボード（図示せず。）を用いて入力された、視聴したい上記コンテンツのタイトルコード１７０９を、ネットワークを介して鍵発行センター装置１７０７の制御部１７０７ａに送信する。なお、上記タイトルコードは、テレビジョン装置１７３０の画面に従って選択することにより入力してもよいし、直接キーボードから入力してもよいし、リモートコントローラー等から入力してもよい。従って、タイトルコードは、ユーザが独自に入手していてもよいし、第１暗号化コンテンツとともにＣＡＴＶデコーダ１７０６に送られてきてもよいし、番組案内などの形態で第１暗号化コンテンツとは別の時刻に予め送られていてもよい。

【０１７４】鍵発行センター装置１７０７の制御部１７０７ａは、ＣＡＴＶデコーダ１７０６のシステムＩＤと、上記コンテンツのタイトルコードとに基づいて、時間制限情報メモリ１７１０内の対応する時間制限情報を参照して、対応する鍵（Ｋ）１７１２を生成して、ＣＡＴＶデコーダ１７０６の第１暗号デコーダ１７１３にネットワークを介して送信する。なお、時間制限情報により、同一のコンテンツを時刻を変えて複数回放送する場合を区別することができる。ここで、第１復号鍵をＦＫとし、ＣＡＴＶデコーダ１７０６のシステムＩＤをＤＩＤとし、時間制限情報をＴＩＭＥとし、コンテンツのタイトルコードをＴとするとき、鍵（Ｋ）１７１２は、次式の関係を満たしている。

【０１７５】

【数１１】ＦＫ＝Ｋ＊Ｔ＊ＤＩＤ＊ＴＩＭＥ

【０１７６】第１暗号デコーダ１７１３は、第１復号鍵（ＦＫ）と、鍵発行センター装置１７０７から送信されてくる上記鍵（Ｋ）１７１２と、上記コンテンツのタイトルコードと、システムＩＤと、時間制限情報とが上述の関係を満たしており、かつ時間制限情報がクロック回路１７２５からの現在時刻情報の条件を満たしていれば、第１暗号化コンテンツ１７０５を復号することができる。ここで、第１暗号化コンテンツ１７０５が画像信号の場合は、デスクランブルされた画像信号が第１暗号化デコーダ１７１３からテレビジョン装置１７３０に出力され、ユーザはコンテンツをテレビジョン装置１７３０で視聴できる。ここで、第１暗号化デコーダ１７１３の復号化処理は次式のように表記される。

【０１７７】

【数１２】

Ｃ［ＦＫ］＃（Ｋ＊Ｔ＊ＤＩＤ＊ＴＩＭＥ）

＝Ｃ［ＦＫ］＃ＦＫ
＝Ｃ

【０１７８】次に、上記コンテンツを光ディスク１６０１に記録する方法を説明する。光ディスク１６０１にコンテンツを記録する際には、ＣＡＴＶデコーダ１７０６にて復号化されていない、第１暗号化コンテンツ１７０５が、ＣＡＴＶ会社装置１７０１の第１暗号化エンコーダ１７０４から光ディスク記録再生装置１７１４の記録回路１７１７に送信される。記録回路１７１７は、受信された第１暗号化コンテンツ１７０５のデータを、例えば公知の８／１６変調方式などの変調方式を用いてディジタル変調し、変調後のディジタルデータは、光ピックアップ（図示せず。）により光ディスク１６０１に記録される。従って、光ディスク１６０１に暗号化されて記録された上記コンテンツを再生するためには、第１暗号化コンテンツ１７０５を復号する必要がある。

【０１７９】光ディスク記録再生装置１７１４は、ＢＣＡ再生回路１７２０により再生された、光ディスク１６０１のディスクＩＤ信号１７１５と、例えばキーボード（図示せず。）を用いて入力された、再生したい上記コンテンツのタイトルコード１７１６とを、ネットワークを介して鍵発行センター装置１７０７の制御部１７０７ａに送信する。なお、ディスクＩＤを送るタイミングは、鍵発行センター装置１７０７とアクセスする際に送ってもよいし、もしくは、視聴の際に、タイトルコードと一緒に送ってもよい。

【０１８０】また、ディスクＩＤの送信方法として、図２２に示すように光ディスク１６０１のＢＣＡ１６０４を再生して、ＢＣＡ再生回路１７２０の出力信号を直接鍵発行センター装置１７０７に送る方法を上記で開示しているが、本発明はこれに限らず、下記の方法を用いてもよい。例えばディスク起動時などの、鍵発行センター装置１７０７とのアクセス以前に、ＢＣＡ１６０４のデータを再生して、光ディスク記録再生装置１７１４又はＣＡＴＶデコーダ１７０６のメモリ（図示せず。）に保管しておき上記タイミングで鍵発行センター装置１７０７の制御部１７０７ａに送信してもよい。さらに、ディスクＩＤが、ラベルなどの形態で視覚的にも認識できる場合には、キーボードから入力してもよいし、ラベルがバーコードになっている場合にはバーコードリーダーから読みとってもよい。

【０１８１】鍵発行センター装置１７０７の制御部１７０７ａは、光ディスク１６０１のディスクＩＤ信号１７１５及びコンテンツのタイトルコード１７１６に対応する鍵（ＤＫ）１７１８を生成して、光ディスク記録再生装置１７１４の鍵情報記録回路１７１９に送信する。ここで、第１復号鍵をＦＫとし、光ディスク１６０１のディスクＩＤ信号１７１５をＢＣＡＳとし、コンテンツのタイトルコード１７１６をＴとするとき、鍵（ＤＫ）は、次式の関係を満たしている。

【０１８２】
【数１３】ＦＫ＝ＤＫ＊ＢＣＡ＊Ｔ

【０１８３】光ディスク記録再生装置１７１４の鍵情報記録回路１７１９に入力された鍵（ＤＫ）は、例えば公知の８／１６変調方式などの変調方式を用いてディジタル変調され、変調後のディジタルデータが光ピックアップ（図示せず。）により光ディスク１６０１の鍵情報記録領域１６０５に記録される。なお、鍵（ＤＫ）は鍵情報記録領域１６０５に、同一の鍵が複数個記録されてもよい。同一の鍵が複数個記録されることにより、鍵情報記録領域１６０５の記録膜が劣化した場合や、光ディスク１６０１に傷がついた場合に鍵（ＤＫ）を保護することができ、いずれか１つの鍵（ＤＫ）のデータを再生することができれば、コンテンツを復号できる。

【０１８４】また、本実施形態では、鍵情報記録領域１６０５はユーザデータ領域１６０３の内周側に設けられているが、ユーザデータ領域１６０３の外周側にあっても良く、内周側と外周側の両方に設けられていてもよい。外周側に設けられることにより、より多くの鍵（ＤＫ）を記録することが可能となる。また、鍵情報記録領域が複数個、分散して設けられることにより、１つの鍵情報記録領域が再生できなくなった場合でも、他の鍵情報記録領域により鍵（ＤＫ）を保護することができる。

【０１８５】一方、光ピックアップから出力されるレーザ光が光ディスク１６０１の上記コンテンツが記録された領域を照射し、その反射光が光ピックアップに入射する。光ピックアップは入射する反射光を光電変換し、光電変換された再生信号をデータ再生部１７２１に出力する。これに応答して、データ再生部１７２１は、入力された再生信号を暗号化ディジタルデータにＡ／Ｄ変換して第２暗号デコーダ１７２２に出力する。さらに、光ピックアップから出力されるレーザ光は光ディスク１６０１のＢＣＡ６０４を照射し、その反射光が光ピックアップに入射する。光ピックアップは入射する反射光を光電変換し、光電変換された再生信号をＢＣＡ再生回路１７２０に出力する。これに応答して、ＢＣＡ再生回路１７２０は、入力される再生信号に基づいてディスクＩＤ信号１７１５を再生して、暗号デコーダ１７２２に出力する。さらに、光ピックアップから出力されるレーザ光は光ディスク１６０１の鍵情報記録領域１６０５を照射し、その反射光が光ピックアップに入射する。光ピックアップは入射する反射光を光電変換して再生信号を鍵情報再生部１７２３に出力し、これに応答して、鍵情報再生部１７２３は、入力される再生信号に基づいて鍵（ＤＫ）のデータを生成して、第２暗号デコーダ１７２２に出力する。

【０１８６】なお、鍵発行センター装置１７０７に対してアクセスしてすぐにコンテンツを再生する際は、鍵情報記録回路１７１９は、鍵（ＤＫ）を鍵情報記録領域１６０５に記録する前に、直接に第２暗号デコーダ１７２

２に入力してもよい。このようにすることにより、再生を開始するまでの時間を短縮することができる。暗号デコーダ１７２２は、入力されたディスクＩＤ信号１７１５と、鍵（ＤＫ）と、上記コンテンツのタイトルコード１７１６とからなる復号鍵とを用いて、暗号化されたコンテンツの復号を行う。第２暗号デコーダ１７２２の復号化処理は次式で表される。コンテンツが画像信号の場合は、例えばＭＰＥＧ信号が伸長されて、画像信号の出力信号１７２４が第２暗号デコーダ１７２２から出力される。

【０１８７】

【数１４】

Ｃ［ＦＫ］＃（ＤＫ＊ＢＣＡ＊Ｔ）
＝Ｃ［ＦＫ］＃ＦＫ
＝Ｃ

【０１８８】本実施形態において、鍵発行センター装置１７０７の制御部１７０７ａから鍵信号を受信するときに課金されるとすると、視聴するときと、光ディスク１６０１に記録したコンテンツを初めて再生するときに別々に課金され、光ディスク１６０１に記録しただけでは課金されない。従って、視聴と光ディスク１６０１への記録の両方に対してまとめて課金する場合に対して、視聴はしたいが光ディスク１６０１に記録する必要がないユーザや、光ディスク１６０１に記録したいが、放送されるときに視聴する必要がないユーザにとっては課金される金額を安くすることができる。また、光ディスク１６０１に記録しただけでは課金されないので、ユーザは視聴した後で、再度視聴するために光ディスク１６０１を再生するための鍵を受け取るかどうかを決定することができる。以上の実施形態においては、鍵（ＤＫ）は鍵発行センター装置１７０７の制御部１７０７ａからネットワークを介して受信する方法を用いているが、本発明はこれに限らず、コンテンツのタイトルとディスクＩＤ番号を電話等で口頭で伝えることにより、口頭で受け取ってキーボードから入力してもよい。

【０１８９】次に、鍵情報記録領域１６０５に鍵（ＤＫ）が記録された光ディスク１６０１を鍵発行センター装置１７０７とのアクセス終了後に再生する場合について説明する。まず、光ピックアップから出力されるレーザ光が光ディスク１６０１の上記コンテンツが記録された領域を照射し、その反射光が光電変換を行う光ピックアップを介してデータ再生部１７２１に入力される。これに応答して、データ再生部１７２１は暗号化されたコンテンツのデータを第２暗号デコーダ１７２２に出力する。一方、光ピックアップから出力されるレーザ光は光ディスク１６０１のＢＣＡ１６０４を照射し、その反射光が光電変換を行う光ピックアップを介してＢＣＡ再生回路１７２０に入力される。これに応答して、ＢＣＡ再生回路１７２０は入力される再生信号に基づいてディスクＩＤ信号１７１５を生成して第２暗号デコーダ１７２２に出力する。

【０１９０】さらに、光ピックアップから出力されるレーザ光は光ディスク１６０１の鍵情報記録領域１６０５を照射し、その反射光が光電変換を行う光ピックアップを介して鍵情報再生部１７２３に入力される。これに応答して、鍵情報再生部１７２３は入力される再生信号に基づいて鍵（ＤＫ）のデータを生成して第２暗号デコーダ１７２２に出力する。第２暗号デコーダ１７２２は、入力されたディスクＩＤ信号１７１５と、鍵（ＤＫ）と、上記コンテンツのタイトルコード１７１６からなる復号鍵を用いて、データ再生部１７２１から出力される、暗号化されたコンテンツの復号を行う。第２暗号デコーダ１７２２の復号化処理は次式で表される。コンテンツが画像信号の場合は、例えばＭＰＥＧ信号が伸長されて、画像信号が第２暗号デコーダ１７２２から出力される。

【０１９１】

【数１５】

Ｃ［ＦＫ］＃（ＤＫ＊ＢＣＡ＊Ｔ）
＝Ｃ［ＦＫ］＃ＦＫ
＝Ｃ

【０１９２】鍵情報記録領域１６０５に鍵（ＤＫ）のデータが一度記録されることにより、鍵発行センター装置１７０７とのアクセスをすることなく、常に上記暗号化コンテンツを再生することができる。また、復号化処理に必要な復号鍵は全て光ディスク１６０１に記録されているので、上記光ディスク１６０１は、ＢＣＡ再生回路１７２０と、鍵情報再生部１７２３と、第２暗号デコーダ１７２２とを有する任意の光ディスク記録再生装置で再生することができる。

【０１９３】さらに、上記暗号化コンテンツをディスクＩＤの異なる光ディスク１６０１にコピーして再生しようとした場合には、ＢＣＡ再生回路１７２０から上記光ディスク１６０１とは異なるディスクＩＤ信号が出力されるので、暗号化されたコンテンツを復号することができず、コンテンツはコピーされても再生されない。ただ、この場合にも、コンテンツのタイトルとディスクＩＤをネットワークもしくは口頭で鍵発行センターに伝えることにより、課金の後、復号鍵を受け取ってもよい。このように、暗号化されたコンテンツを別の光ディスク１６０１にコピーされても、不正に再生されることはなく、暗号化されたコンテンツをコピーした光ディスク１６０１を再生する際には必ず課金が伴うことから著作権を保護することができる。

【０１９４】図２３は、第５の実施形態に係るＩＤ付与テーブルの構成を示す表であり、システムＩＤやディスクＩＤが異なる場合の第１暗号デコーダ１７１３に入力される鍵（Ｋ）と、鍵情報記録回路１７１９に入力される鍵（ＤＫ）とを整理して示したものである。図２３において、Ｔ１、Ｔ２、Ｔ３は異なるコンテンツのタイト

ルコードであり、ＦＫ１、ＦＫ２、ＦＫ３はそれぞれＴ１、Ｔ２、Ｔ３のタイトルコードを有する暗号化コンテンツを復号するための復号鍵である。また、ＤＩＤ１、ＤＩＤ２、ＤＩＤ３はそれぞれ異なるＣＡＴＶデコーダ１７０６のシステムＩＤであり、ＢＣＡＳ１、ＢＣＡＳ２、ＢＣＡＳ３はそれぞれ異なる光ディスク１６０１のディスクＩＤである。このとき、ＣＡＴＶデコーダ１７０６に入力される鍵（Ｋｍｎ）は、次式を満足するように決定される。

【０１９５】

【数１６】ＦＫｎ＝Ｋｍｎ＊Ｔｎ＊ＤＩＤ＊ＴＩＭＥｎ

【０１９６】また、光ディスク記録再生装置１７１４に入力される鍵（ＤＫｍｎ）は、次式を満足するように決定される。

【０１９７】

【数１７】ＦＫｎ＝ＤＫｍｎ＊ＢＣＡｍ＊Ｔｎ

【０１９８】図２３に示すように、コンテンツが異なるときはもちろんのこと、コンテンツが同じ場合でも、異なるＣＡＴＶデコーダ１７０６、異なる光ディスク、異なる放送時間毎に鍵発行センター装置１７０７から入手する鍵情報は異なることから細部にわたる著作権の保護が可能になる。同様に、コンテンツが同じでもシステムＩＤ、ディスクＩＤ、時間情報が異なれば鍵情報が異なることから、ＣＡＴＶ会社装置１７０１は、ユーザ毎に暗号化コンテンツを変える必要がなく、１つのコンテンツに対して１つの暗号化コンテンツを準備すればよい。これにより放送時のシステムを簡単にでき、低コストで、大量の視聴者へのコンテンツの提供が可能になる。

【０１９９】なお、本実施形態では、ケーブルテレビジョンのヘッドエンドからのコンテンツを放送する場合について説明したが、電波による放送でも同様である。

【０２００】＜第３乃至第５の実施形態の効果＞本実施形態に係る光ディスクは、第１のディスク情報が記録されている第１の情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２の情報領域と、光ビームを照射することにより情報の記録が可能なユーザデータ領域を有する。従って、従来技術の光ディスクに、上記光ディスクを識別する情報を付加することにより、光ディスクの管理を容易に実現することができる。ここで、上記第２の情報領域は、好ましくは、上記第１の情報領域内に記録されているものであり、上記第１の情報領域を再生する光ピックアップによって再生することができる。また、上記第２の情報領域は、上記第１の情報領域内の記録膜を、半径方向に長い形状でかつ複数個のトリミング領域が形成されるように、部分的に除去することにより記録されているものであり、容易に上記第２のディスク情報が改ざんされることを防止することができる。

【０２０１】また、本実施形態に係る暗号化コンテンツの記録方法によれば、第１のディスク情報が記録されている第１の情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２の情報領域と、光ビームを照射することにより情報の記録が可能なユーザデータ領域を有する光ディスクの上記ユーザデータ領域にコンテンツのデータを記録する際に、少なくとも上記第２のディスク情報を用いた演算によりコンテンツのデータを復号して再生することができるように、コンテンツのデータを暗号化して記録する。従って、特定の１枚の光ディスクにしか存在しない光ディスクの識別情報を用いて、コンテンツを暗号化することにより、コンテンツの不正なコピーを防止することができ、著作権が保護できるという特有の効果がある。

【０２０２】さらに、本実施形態に係る光ディスクは、ユーザデータ領域内に、暗号化されて記録されたコンテンツを解読するための鍵情報を記録する鍵情報記録領域を有する。従って、暗号化されて記録されたコンテンツを解読する際に鍵情報が必要なシステムにおいて、鍵情報記録領域に鍵情報が一度記録されることにより、再生する度に鍵情報を入力する必要がなくなるという特有の効果がある。

【０２０３】またさらに、本実施形態に係る暗号化コンテンツの記録方法によれば、第１のディスク情報が記録されている第１の情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２の情報領域と、光ビームを照射することにより情報の記録が可能なユーザデータ領域と、ユーザデータ領域内に、暗号化されて記録されたコンテンツのデータを解読するための鍵情報を記録する鍵情報記録領域を有する光ディスクの上記ユーザデータ領域にコンテンツを記録する際に、少なくとも上記第２のディスク情報と、上記鍵情報を用いた演算によりコンテンツのデータを復号して再生することができるようにコンテンツのデータを暗号化して記録する。従って、暗号化されたコンテンツのデータを別の光ディスクにコピーされても、不正に再生されることはなく、暗号化されたコンテンツのデータをコピーした光ディスクを再生する際には必ず課金が伴うことから著作権を保護することができる。

【０２０４】ここで、第１のディスク情報は、好ましくは、微少な凹凸ピットにより構成され、光ディスクを識別するための第２のディスク情報が、上記凹凸ピット上に記録される。従って、容易に第２のディスク情報が改ざんされることを防止することができる。さらに、好ましくは、上記第１のディスク情報と第２のディスク情報が隣接するように形成される。これにより、上記第１のディスク情報を再生する際に、第２のディスク情報も続けて再生することができ、もしくは第２のディスク情報を再生する際に、第１のディスク情報を続けて再生することができるので、例えば光ディスクを起動する際にＣＰＵが速やかにディスクを識別するための第２のディスク情報を入手し、暗号化されたコンテンツを記録するた

めの処理を早めることが可能になる。

【０２０５】また、本実施形態に係る暗号化データの記録方法によれば、コンテンツが同じでもシステムＩＤ、ディスクＩＤ、時間情報が異なれば鍵情報が異なることから、ＣＡＴＶ会社装置７０１は、ユーザ毎に暗号化コンテンツを変える必要がなく、１つのコンテンツに対して１つの暗号化コンテンツを準備すればよく、これにより放送時のシステムを簡単にでき、低コストで、大量の視聴者へのコンテンツの提供が可能になる。

【０２０６】＜第３及び第５の実施形態の変形例＞以上の第３と第５の実施形態においては、図１６及び図２１に示すように、トリミング領域１１０５，１６０６はそれぞれ、コントロールユーザデータ領域１１０２，１６０２内の内周部に位置するＢＣＡ１１０４，１６０４に形成しているが、本発明はこれに限らず、それぞれ第３と第５の実施形態の変形例に係る光ディスク１１０１ａ，１６０１ａのデータ記録領域を示す図２４及び図２５に示すように、コントロールユーザデータ領域１１０２，１６０２から光ディスクの内周側にはみ出るように記録膜をトリミングしてトリミング領域１１０５ａ，１６０６ａを形成してもよい。すなわち、ＢＣＡ１１０４ａ，１６０４ａはそれぞれ、コントロールユーザデータ領域１１０２，１６０２内に含まれず、コントロールユーザデータ領域１１０２，１６０２の内周部から、コントロールユーザデータ領域１１０２，１６０２の内側にはみ出るように配置されて形成される。この変形例において、ＢＣＡ１１０４ａ，１６０４ａをこのように形成するのは、フォーカスサーボ回路の不安定性によりレーザ光のビームのスポットの径が変化する場合のマージンを考慮しているためである。この変形例においても、コントローラユーザデータ領域１１０２，１６０２の外側にユーザデータ領域１１０３，１６０３が存在しているので、これらのユーザデータ領域１１０３，１６０２に記録されたデータを破壊しないように保護するために、トリミング領域１１０５ａ，１６０６ａが配置されて形成される。

【０２０７】＜第６の実施形態＞図２６は、本発明に係る第６の実施形態である光ディスク内のユーザデータ領域の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。本実施形態において、光ディスクは、例えば、ＤＶＤ－ＲＡＭなどの記録型光ディスクである。

【０２０８】図２６に示すように、ユーザデータ領域２１５０は、セクタヘッダ領域２１０１と、メインデータ領域２１０２と、誤り検出コード２１０３とから構成される。セクタヘッダ領域２１０１には、セクタの位置を示すセクタアドレス２１０４と、メインデータ領域２１０２に記録されるデータに関する著作権制御情報（スクランブルフラグ、コピー制御情報などを含む。）が記録される著作権制御情報２１０５とが記録されるとともに、セクタヘッド領域２１０１は、メインデータ領域２１０２のデータに暗号が施されている場合に復号するための復号鍵領域２１０６を含む。また、メインデータ領域２１０２は、非暗号化コンテンツ２１０７が記録される領域と、暗号化コンテンツ２１０８が記録される領域とに分割され、非暗号化コンテンツ２１０７は、ＭＰＥＧにおける同期パターンや、各種制御情報などの後続するデータの制御情報を含む。さらに、暗号化コンテンツ２１０８は、主に著作権保護を必要とするＡＶデータなどが暗号化されたコンテンツのデータを含む。

【０２０９】復号鍵領域２１０６には、後続するメインデータ領域２１０２を再生するための復号鍵が所定のサイズを有する複数の分割された復号鍵（以下、分割復号鍵という。）に分割されて記録される。例えば、４バイトの１つの復号鍵領域に対して復号鍵が８バイトである場合、８バイトの復号鍵を各４バイトの分割復号鍵に分割し、論理的に連続する２つのセクタの復号鍵領域２１０６，２１０９にそれぞれ、分割された２つの分割復号鍵を記録する。このようなユーザデータ領域の再生時には、論理的に連続する（ただし、欠陥等により使用不可能なセクタはスキップする。）複数のセクタの復号鍵領域２１０６，２１０９から分割された複数の分割復号鍵を取得し、取得された必要数の分割復号鍵をデータ連結器２１１１にて連結し、再生に必要な暗号化復号鍵（８バイト）を得る。暗号化復号鍵（８バイト）を得ることのできたセクタのメインデータ領域２１０２に記録されたデータに対して、それぞれの著作権制御情報２１０５の内容に従って、復号器２１１４を用いて復号化処理を実行する。

【０２１０】さらに、より暗号の強度を高めるために、復号鍵に対して暗号化を施すことも可能であるし、暗号の結果が一定とならないように、データ中の情報である復号鍵変換データを鍵に加えることにより、同一の暗号鍵であっても、異なる暗号結果を提供することも可能である。具体的には、図２６に示すように、データ連結器２１１１から出力される暗号化復号鍵が鍵復号器２１１２に入力され、鍵復号器２１１２は、入力された暗号化復号鍵を、所定のディスク鍵を用いて、ダミーデータであるパディングデータ（１バイト）と復号鍵（７バイト）に復号化して鍵変換器２１１３に出力する。ここで、ディスク鍵は、例えば、光ディスクに記録された暗号化ディスク鍵を、所定のマスター鍵である秘密鍵を用いて、ディスク鍵復号器（図示せず。）により復号することにより取得される。次いで、鍵変換器２１１３は、メインデータ領域２１０２から読み出した復号鍵変換データ２１１０を、上記鍵復号器２１１２から出力される復号鍵を用いて、例えば乗算や除算、所定の重み係数を用いた演算などの所定の変換演算によりデータ変換することによりコンテンツ復号鍵（７バイト）を生成して復号器２１１４に出力する。そして、復号器２１１４は、

メインデータ領域２１０２から読み出したコンテンツのデータを、上記鍵変換器２１１３から出力されるコンテンツ復号鍵（７バイト）を用いて復号することにより、復号化されたコンテンツのデータを生成して出力する。なお、復号鍵変換データ２１１０としては、コピー世代管理情報や、アナログのマクロビジョン制御フラグなどの改ざんがされることによりデータの不正利用がすぐに検出可能であるようなデータを利用することが好ましい。

【０２１１】図２７は、第６の実施形態に係る光ディスクにおいて、ユーザデータ領域への著作権制御情報と復号鍵の配置と、メインデータ領域への暗号化コンテンツの配置を示すブロック図である。図２７に図示されたユーザデータ領域２１５０の一例においては、復号鍵領域が、４バイトの分割復号鍵を有する第１の復号鍵領域２２０１と、４バイトの分割復号鍵を有する第２の復号鍵領域２２０２とに分割されて配置されている。このため、これらの２つのセクタに記録する暗号化コンテンツの大きさによらず、複数のセクタ（図２７では２つのセクタ）が使用されることとなる。この場合、未使用の領域には、ダミーデータが補完データとして記録される。図２７の例では、１セクタ分の暗号化コンテンツ２２０４しかない場合には、１セクタ分の補完データ２２０３が記録される。

【０２１２】図２８は、第６の実施形態に係る光ディスクにおいて、エラー訂正の単位が複数のセクタにまたがる場合の配置を示すブロック図である。例えば、光ディスクがＤＶＤである場合、１６セクタのエラー訂正コードの単位ブロック（以下、ＥＣＣブロックという。）を用いることにより、エラー訂正の能力を高めている。このため、データの記録や再生を行う際には、ＥＣＣブロック単位での記録が必要となる。復号鍵を任意の複数の分割復号鍵に分割して記録を行ったとすると、１つの復号鍵が複数のエラー訂正ブロックにまたがって記録される場合が発生する。再生の際には、分割された複数の分割復号鍵のすべてを再生する必要があるため、暗号化コンテンツのデータを記録したセクタ以外にも、復号鍵を記録した直前のＥＣＣブロックまでも再生する必要がある。図２８の例では、復号鍵を分割するときの分割数をＥＣＣブロックのセクタ数の約数に設定することを特徴としている。これにより、分割された複数の分割復号鍵がＥＣＣブロックにまたがって記録されることがなくなる。さらに、１つのＥＣＣブロック内で使用する復号鍵として、１種類の復号鍵のみを用い、記録するＡＶデータがＥＣＣブロックに満たない場合には、補完データ、並びに補完セクタを配置することによって、再生時に不要なセクタのデータを光ディスクから読み出すことを防止することができる。

【０２１３】＜第７の実施形態＞図２９は、本発明に係る第７の実施形態である光ディスク内のリードイン領域２４０１とユーザデータ領域２４０２の構成と、リードイン領域２４０１とユーザデータ領域２４０２のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。

【０２１４】図２９において、図２６の第６の実施形態と同様に、リードイン領域２４０１とユーザデータ領域２４０２はそれぞれ、セクタヘッダ領域２１０１と、メインデータ領域２１０２と、誤り検出コード２１０３とを有するセクタから構成される。セクタヘッダ領域２１０１には、セクタの位置を示すセクタアドレス２１０４と、メインデータ領域２１０２に記録されるデータに関する著作権制御情報（スクランブルフラグ、コピー制御情報などを含む。）が記録される著作権制御情報２１０５とが記録されるとともに、セクタヘッダ領域２１０１は、メインデータ領域２１０２のデータに対して暗号が施されている場合に復号するための復号鍵を参照するための、復号鍵の記録位置（メインデータ領域２１０２内の復号鍵テーブル２４０４での記録位置又は格納位置をいう。）を示す鍵インデックスを記録する鍵インデックス領域２４０３を含む。ユーザデータ領域２４０２に記録された暗号化コンテンツを復号するための復号鍵は、テーブル形式で書き換え可能なリードイン領域２４０１に復号鍵テーブル２４０４の形式で記録される。鍵インデックス領域２４０３に記録される鍵インデックスによりリードイン領域２４０１に記録された復号鍵が参照される。図２６に図示された第６の実施形態と同様に、上記参照された復号鍵は、所定のディスク鍵を用いる鍵復号器２１１２によりパディングデータと復号鍵（又はタイトル鍵）とに復号された後、上記復号された復号鍵（又はタイトル鍵）は、復号鍵変換データを用いる鍵変換器２１１３によりコンテンツ復号鍵に変換されて復号器２１１４に出力される。復号器２１１４は、暗号化されたコンテンツのデータを、コンテンツ復号鍵を用いて復号することにより、復号化コンテンツのデータを生成して出力する。

【０２１５】以上のように構成された第７の実施形態に係る光ディスクと光ディスク再生装置においては、セクタヘッダ領域２１０１内にある鍵インデックス領域２４０３に参照用の鍵インデックスを記録することにより、鍵インデックス領域２４０３のサイズとは独立に復号鍵テーブル２４０４の復号鍵サイズを割り当てることができる。また、復号鍵テーブル２４０４のサイズを割り当てた後も、鍵インデックス領域２４０３内の鍵インデックスで示される復号鍵テーブル２４０４から連続して複数の復号鍵を使用することにより、自由なサイズの復号鍵を利用することができる。

【０２１６】図３０（ａ）は第７の実施形態に係る光ディスク内のリードイン領域２４０１のメインデータ領域２１０２において、復号鍵の初期値で未記録状態を表示する場合のデータ構成を示すブロック図である。図３０

（ａ）において、光ディスクのフォーマット時などにおいて記録される復号鍵の初期値として、鍵として使用しない既知の固定値（例えば、オール０などのデータ）である未記録状態データ２５０１を記録し、これにより、復号鍵の未記録状態を示す。

【０２１７】図３０（ｂ）は第７の実施形態に係る光ディスク内のリードイン領域２４０１のメインデータ領域２１０２において、復号鍵状態テーブルで記録状態を表示する場合のデータ構成を示すブロック図である。図３０（ｂ）においては、図３０（ａ）に図示された復号鍵と同様に、インデックスにより参照可能なテーブル形式の復号鍵状態テーブル２５０２をリードイン領域２４０１に配置し、復号鍵の記録状態を記録状態データ２５０３として以下のように記載している。

（１）０ｘ００：未使用、
（２）０ｘ０１：領域予約、
（３）０ｘ０３：鍵記録済み、
（４）その他：予約済み。

ここで、０ｘは、それに続く文字について１６進数表示を示す。

【０２１８】図３１は、第７の実施形態に係る光ディスクにおいて復号鍵の配置を示すブロック図である。図３１の例では、復号鍵の信頼性を高めるためにディスク上への復号鍵領域の配置を工夫している。通常、ユーザデータ領域２６０２においては欠陥管理が行われるため、書き込み不良が発生した場合には、代替領域等へ交代処理が行われる。しかしながら、リードイン領域２６０１では、上記のような欠陥管理は行われない。このため、書き込み不良や読み出し不良などの発生により、ＡＶデータの再生に必要な復号鍵が利用不能となり、さらには光ディスクそのものが利用不能となる場合がある。従って、異なる複数のＥＣＣブロックにわたって、合計複数の復号鍵を記録しておくことが望ましい。また、近接した領域に複数の復号鍵を記録した場合、傷や埃等により複数記録したものがすべて読めなくなる場合がある。このため、図３１に示すように、リードイン領域２６０１とリードアウト領域２６０３においてそれぞれ、光ディスクの内周側と外周側といったようなレイアウト上離れた位置に各復号鍵を記録しておくことがより好ましい。

【０２１９】なお、図２９の実施形態においては、復号鍵領域をリードイン領域２４０１，２６０１に配置している。これは、ユーザデータ領域２６０２が通常のリードコマンドやライトコマンドでアクセス可能な領域であることを考慮し、パーソナルコンピュータのドライブ装置などからアクセスするときの安全性を高めるためである。従って、これらをユーザデータ領域２６０２に配置しても、同様の効果を得ることができる。

【０２２０】＜第８の実施形態＞図３２は、本発明に係る第８の実施形態である光ディスクのデータをファイル管理システムにより管理するときのデータ構成を示すブロック図である。図３２の例では、ファイルシステムの構造に基づいて、所望のファイルが格納されたセクタアドレスを管理している。

【０２２１】国際標準化機構によりＩＳＯ１３３４６において規定されたファイルシステムの構造では、書き換え可能型光ディスクに対応するために、ファイルの記録位置はファイルエントリと呼ばれる情報を用いて管理される。図３２に示すように、例えば、ファイル（１）２７０３の記録位置のデータは、ファイル管理情報領域２７５１内のファイルエントリ（１）２７０１として格納され、ファイル（２）２７０４の記録位置のデータはファイルエントリ（２）２７０２として格納される。各ファイルは、光ディスク上で連続した複数のセクタの領域を管理するエクステント２７０５，２７０６で構成される。光ディスク上には、ファイルエントリが示すメインデータ領域２１０２において、第７の実施形態で示した暗号化コンテンツが記録され、また、復号鍵がリードイン領域２６０１内の復号鍵テーブル２７０７に記録される。暗号化コンテンツが記録されたユーザデータ領域２６０２内のセクタヘッダ領域２１０１には、復号に必要な復号鍵を参照するための記録位置を示すポインタが、鍵インデックス領域２７０８において記録される。なお、本実施形態では、ファイル単位とエクステント単位で復号鍵を管理して記録しているが、本発明はこれに限らず、ファイル単位とエクステント単位とのうちの少なくとも一方で復号鍵を管理して記録してもよい。

【０２２２】上記のようにファイルシステムにより管理される光ディスクにおいて、著作権保護を必要とするコンテンツの記録動作について図３３を用いて説明する。図３３は、第８の実施形態に係るファイル管理システムによって実行される、著作権保護を必要とするコンテンツの記録処理を示す。

【０２２３】暗号化コンテンツの記録の際には、まず、ステップＳ２８０１において、図３０（ｂ）に図示された復号鍵状態テーブル２５０２を読み出して、復号鍵テーブル２７０７の空き領域を調べる。次いで、ステップＳ２８０２において、復号鍵テーブル２７０７の空き領域があるか否かが判断され、ＮＯのときは、暗号化コンテンツに対する復号鍵が記録できないために、ステップＳ２８０７において記録動作を中止して当該コンテンツの記録処理を終了する。一方、ステップＳ２８０２でＹＥＳであるときは、取得済みの復号鍵（又はタイトル鍵）を記録し、また、復号鍵を取得できていない場合には、復号鍵領域の予約を行う。次いで、ステップＳ２８０４では、記録するコンテンツの著作権制御情報（暗号化を行うか否かの情報と、暗号化の種類を示す種別の情報などを含む。）と、鍵インデックス領域２７０８に記録する鍵インデックスの設定を行った後、ステップＳ２８０５においてコンテンツを暗号化してエクステント単位でファイル形式で光ディスク上に記録する。このと

き、ファイル単位で同一の著作権制御情報と鍵インデックスを使用してもよいし、エクステント単位でこれらを切り替えてもよい。すなわち、ステップＳ２８０４及びＳ２８０５において、処理する単位は、ファイル単位と、エクステント単位とのうちの少なくとも一方である。最後に、ステップＳ２８０６において、記録したコンテンツに関する情報に基づいて、上記記録されたデータを管理するためのファイル管理情報の更新を行った後、当該コンテンツの記録処理を終了する。

【０２２４】図３４は、第８の実施形態に係るファイル管理システムによって実行される、コンテンツの再生処理を示すフローチャートである。図３４では、図３３に示した方法によりファイル形式で記録したコンテンツを光ディスクから再生する処理を示す。

【０２２５】ファイルの再生動作を行う際には、再生するファイルが使用している復号鍵テーブルの領域を知るため、ファイル管理情報領域２７５１内のファイルエントリにより示される領域に対する鍵インデックスを取得する。具体的には、ステップＳ２９０１において、ファイル管理情報２７５１から再生するファイルのファイルエントリを読み出して再生することにより取得した後、ステップＳ２９０２において、ファイルエントリにより示される領域のセクタヘッダ領域２１０２から鍵インデックス領域の値を読み出して再生することにより取得する。エクステント単位で異なる暗号を行っている場合には、それぞれのエクステントにおいてセクタヘッダ中の鍵インデックス領域を読み出す。次いで、ステップＳ２９０３において、取得した鍵インデックスにより示される復号鍵テーブル２７０７の復号鍵領域から復号鍵を読み出して再生することにより取得する。さらに、ステップＳ２９０４において、ファイルエントリで示される領域からファイル内のコンテンツのデータを読み出して再生し、再生したコンテンツのデータを復号する。ここで、コンテンツのファイルの再生と復号が終了すれば、当該コンテンツの再生処理を終了する。

【０２２６】図３５は、第８の実施形態に係るファイル管理システムによって実行される、コンテンツの削除処理を示すフローチャートであり、図３５では、図３３に示した方法により記録したファイル形式のコンテンツのデータを削除する動作について示す。

【０２２７】ファイルの削除動作を行う際には、削除するファイルが使用している復号鍵テーブル２７０７の領域を知るため、ファイルエントリにより示される領域に対する鍵インデックスを取得する。具体的には、ステップＳ３００１において、ファイル管理情報領域２７５１内のファイル管理情報から削除するファイルのファイルエントリを取得した後、ステップＳ３００２においてファイルエントリにより示される領域のセクタヘッダから鍵インデックス領域の値を取得する。ここで、エクステント単位で異なる暗号を行っている場合には、それぞれのエクステントにおいてセクタヘッダ中の鍵インデックス領域を読み出す。次いで、ステップＳ３００３において、取得した鍵インデックスにより示される復号鍵テーブル２７０７の復号鍵領域から復号鍵を開放した（ここで、復号鍵の開放とは、当該復号鍵を当該テーブルから削除することをいう。）後、ステップＳ３００４において削除するファイルの書き込み位置を示すファイルエントリをファイル管理情報から削除して、当該コンテンツの削除処理を終了する。従来のファイルシステムでは、ファイルを削除する際にファイルエントリのみの削除を行っていたが、復号鍵と暗号化コンテンツの記録セクタが別の領域に記録されているために、別の領域に記録された復号鍵を削除できない。上述の実施形態においては、ファイルエントリの削除に先立って、セクタヘッダ領域中の鍵インデックスの示す復号鍵を復号鍵テーブル２７０７から削除することにより、光ディスク上での復号鍵の管理を行っている。

【０２２８】＜第９の実施形態＞図３６は、本発明に係る第９の実施形態である光ディスクシステムの構成を示すブロック図であり、この光ディスクシステムは、光ディスク３１００に著作権保護を必要とするコンテンツを記録及び再生する情報処理システムである。当該光ディスクシステムは、エンコード装置３１０１と、光ディスク装置３１０２と、デコード装置３１０３と、パーソナルコンピュータ３１０４とを備えて構成される。

【０２２９】エンコード装置３１０１は、コンテンツのデータを格納するコンテンツメモリ３１３１と、上記コンテンツのデータをＭＰＥＧフォーマットの形式で符号化する符号化回路３１３２と、暗号鍵を格納する暗号鍵メモリ３１３３と、符号化されたコンテンツのデータを暗号鍵を用いて暗号化するとともに復号鍵を生成して復号鍵メモリ３１１１に格納する暗号回路３１３４と、復号鍵を格納する復号鍵メモリ３１１１と、復号鍵をバス暗号化するバス暗号回路３１１２と、パーソナルコンピュータ３１０４のインターフェース３１２２にＰＣＩバス３１５１を介して接続され暗号化されたコンテンツのデータや復号鍵を送信するインターフェース３１２４とを備える。また、光ディスク装置３１０２は、複数の復号鍵を格納する復号鍵テーブルメモリ３１１３と、バス暗号及び復号回路３１１４と、光ディスク３１００に対してデータを記録するとともに光ディスク３１００からデータを読み出して再生する記録再生回路３１１９と、パーソナルコンピュータ３１０４のインターフェース３１２１とＳＣＳＩバス３１５２を介して接続されデータや信号の送信及び受信並びに信号変換、プロトコル変換などの処理を実行するインターフェース３１２０とを備える。なお、ＳＣＳＩバス３１５２はＡＴＡＰＩバスであってもよい。ここで、バス暗号化及びバス復号化とはそれぞれ、ＰＣＩバス３１５１やＳＣＳＩバス３１５２上で暗号鍵や復号鍵を暗号化して送信し受信するために

用いる暗号化処理、及び復号化処理をいう。

【０２３０】さらに、パーソナルコンピュータ３１０４は、その動作を制御する制御部３１３０と、複数のバス暗号化復号鍵を格納するバス暗号化復号鍵テーブルメモリ３１１５と、上記複数のバス暗号化復号鍵に対応する複数の復号鍵ステータス（復号鍵の記録状態を示し、具体的には、未使用、領域予約、鍵記録済み、予約済みなどを示す。）のデータを格納する復号鍵状態テーブルメモリ３１１６と、光ディスク装置３１０２のインターフェース３１２０とＳＣＳＩバス３１５２を介して接続されデータや信号の送信及び受信並びに信号変換、プロトコル変換などの処理を実行するインターフェース３１２１と、デコード装置３１０３のインターフェース３１２３及びエンコード装置３１０１のインターフェース３１２４とＰＣＩバス３１５１を介して接続されデータや信号の送信及び受信並びに信号変換、プロトコル変換などの処理を実行するインターフェース３１２２とを備える。またさらに、デコード装置３１０３は、パーソナルコンピュータ３１０４のインターフェース３１２２と接続されデータや信号の送信及び受信並びに信号変換、プロトコル変換などの処理を実行するインターフェース３１２３と、インターフェース３１２３によって受信された暗号化復号鍵をバス復号化するバス復号回路３１１７と、復号鍵を格納する復号鍵メモリ３１１８と、インターフェース３１２３によって受信された暗号化コンテンツのデータを復号鍵メモリ３１１８の復号鍵を用いて復号するとともに、ＭＰＥＧフォーマットの復号化処理を行って画像信号や音声信号を生成してディスプレイ装置３１０５に出力する復号化回路３１４１とを備える。

【０２３１】この光ディスクシステムのエンコード装置３１０１においては、符号化回路３１３２は、コンテンツメモリ３１３１に格納され又は入力されるＡＶデータなどのコンテンツのデータをＭＰＥＧのフォーマットの形式で符号化し、暗号回路３１３４は、パーソナルコンピュータ３１０４上でのコンテンツの不正利用を避けるために生成された暗号鍵メモリ３１３３内の暗号鍵を用いて上記符号化されたコンテンツのデータを暗号化し、暗号化されたコンテンツのデータをインターフェース３１２４及びパーソナルコンピュータ３１０４を介して光ディスク装置３１０２に送信する。ここで、暗号化されたコンテンツのデータは、エンコード装置３１０１のインターフェース３１２４からＰＣＩバス３１５１と、パーソナルコンピュータ３１０４のインターフェース３１２２及びインターフェース３１２１と、光ディスク装置３１０２のインターフェース３１２０を介して記録再生回路３１１９に送信される。そして、暗号化されたコンテンツのデータは、光ディスク装置３１０２の記録再生回路３１１９により光ディスク３１００に記録される。また、光ディスク装置３１０２の記録再生回路３１１９は、光ディスク３１００に記録されている暗号化コンテンツのデータを再生して、再生された暗号化コンテンツのデータを、インターフェース３１２０と、パーソナルコンピュータ３１０４のインターフェース３１２１及びインターフェース３１２２と、デコード装置３１０３のインターフェース３１２３を介して復号化回路３１４１に送信する。デコード装置３１０３の復号化回路３１４１は、暗号化コンテンツのデータに対する暗号を復号化しかつＭＰＥＧフォーマットの復号化処理を行い、復号化されたコンテンツの画像信号や音声信号をそれぞれディスプレイ装置３１０５やスピーカ装置（図示せず。）に出力する。

【０２３２】エンコード装置３１０１の暗号回路３１３４は、ＭＰＥＧフォーマットの形式で符号化されたコンテンツのデータに対して、暗号鍵メモリ３１３３内の暗号鍵を用いて暗号化を行うと同時に、再生時に必要な復号鍵を生成して復号鍵メモリ３１１１に格納する。光ディスク３１００には、符号化されたコンテンツのデータと復号鍵を記録する必要があるが、パーソナルコンピュータ３１０４上で復号鍵を平文のまま取り扱う場合には、復号鍵を光ディスク３１００から読み出すことにより、暗号化されたコンテンツのデータの解読が容易になってしまう可能性がある。これを避けるために、エンコード装置３１０１と光ディスク装置３１０２の間で、相互認証を行うとともに相互に共有したバス鍵を用いてバス暗号を行う。

【０２３３】すなわち、具体的には、復号鍵メモリ３１１１内の復号鍵はエンコード装置３１０１のバス暗号回路３１１２によって暗号化が施された後、その暗号化復号鍵は、インターフェース３１２４、ＰＣＩバス３１５１及びインターフェース３１２２を介してパーソナルコンピュータ３１０４のバス暗号化復号鍵テーブルメモリ３１１５に格納される。一方、光ディスク装置３１０２のバス暗号及び復号回路３１１４においては、光ディスク３１００から記録再生回路３１１９により再生された、暗号化復号鍵の復号化が行われた後、復号化された復号鍵は復号鍵テーブルメモリ３１１３に格納される。また、バス暗号及び復号回路３１１４は、例えば更新されたバス暗号化された復号鍵を、バス暗号化復号鍵テーブルメモリ３１１５からインターフェース３１２１、ＳＣＳＩバス３１５２及びインターフェース３１２０を介して受信してバス復号化して復号鍵テーブルメモリ３１１３に格納した後、記録再生回路３１１９を介して光ディスク３１００に記録する。

【０２３４】また、復号鍵状態テーブルは記録再生回路３１１９により光ディスク３１００から再生された後、インターフェース３１２０、ＳＣＳＩバス３１５２及びインターフェース３１２１を介して復号鍵状態テーブルメモリ３１１６に転送されて格納される。さらに、パーソナルコンピュータ３１０４で更新された復号鍵状態テーブルは、復号鍵状態テーブルメモリ３１１６から読み

出されて、インターフェース３１２１、ＳＣＳＩバス３１５２及びインターフェース３１２０を介して記録再生回路３１１９に転送された後、記録再生回路３１１９は受信した復号鍵状態テーブルを光ディスク３１００に記録する。従って、中間に位置するパーソナルコンピュータ３１０４上では、複数のバス暗号化復号鍵を格納するバス暗号化復号鍵テーブル３１１５と復号鍵状態テーブルメモリ３１１６とを用いて、暗号化された復号鍵のみが取り扱われることになり、一層の安全性が確保されることになる。

【０２３５】光ディスク装置３１０２とデコード装置３１０３の間でも同様に復号鍵のバス暗号を行うことにより、一層の安全性が確保される。すなわち、デコード装置３１０３のバス復号回路３１１７は、パーソナルコンピュータ３１０４からインターフェース３１２３を介して受信した暗号化復号鍵を復号して復号鍵メモリ３１１８に格納する。復号化回路３１４１は、復号鍵メモリ３１１８内の復号鍵を用いて暗号化されたコンテンツのデータを復号する。

【０２３６】上述の第７の実施形態に示したように、光ディスク３１００上に暗号化されたコンテンツのデータを復号するための復号鍵をテーブル形式で記録するような場合には、光ディスク装置３１０２上で再生した復号鍵テーブルをバス暗号及び復号回路３１１４によりバス暗号化した後、バス暗号化された復号鍵テーブルのデータをインターフェース３１２０を介してパーソナルコンピュータ３１０４のバス暗号化復号鍵テーブルメモリ３１１５に転送して格納する。コンテンツのデータを記録するときには、パーソナルコンピュータ３１０４が平文で光ディスク３１００に記録されている復号鍵状態テーブルから復号鍵テーブルの空き領域を検索することにより調べ、エンコード装置３１０１から転送されるバス暗号化された復号鍵を空き領域に割り当てる。このとき、バス暗号として復号鍵単位で完結するような暗号（例えば、復号鍵長単位でのブロック暗号）を用いれば、復号鍵ブロックへの割り当て時に、復号鍵の復号し再暗号する必要がない。

【０２３７】なお、光ディスク装置３１００と、光ディスク装置３１０２と、パーソナルコンピュータ３１０４と間で転送されて格納される復号鍵テーブルや復号鍵状態テーブルはそれぞれ、１つのかたまりのブロックのデータであるので、ブロックデータということができる。

【０２３８】コンテンツの再生時の場合も、光ディスク装置３１０２から再生された復号鍵ブロックから再生しようとしているコンテンツの復号化に必要な復号鍵のみを、バス暗号化復号鍵テーブルメモリ３１１５から検索して抜き出し、パーソナルコンピュータ３１０４及びデコード装置３１０３のバス復号回路３１１７を介して復号鍵メモリ３１１８に転送して格納する。そして、復号化回路３１４１は、光ディスク装置３１０２の記録再生回路３１１９によって光ディスク３１００から再生された暗号化されたＡＶデータを、パーソナルコンピュータ３１０４及びインターフェース３１２３を介して受信して、受信された暗号化されたＡＶデータを復号鍵メモリ３１１８内の復号鍵を用いて画像信号や音声信号に復号化して出力する。この場合も、上述のコンテンツの記録時と同様に、バス暗号として復号鍵単位で完結するような暗号（例えば、復号鍵長単位でのブロック暗号）を用いれば、復号鍵ブロックからの復号鍵を抜き取る時に、復号鍵の復号し、再暗号する必要がない。さらに、復号鍵のサイズを大きくする場合には、光ディスク装置３１０２の構成を変更すること無く、複数の復号鍵を割り当てるなどの復号鍵領域の拡張がパーソナルコンピュータ３１０４上で容易かつ安全に行うことができる。

【０２３９】＜第１０の実施形態＞図３７は、本発明に係る第１０の実施形態である光ディスク内のユーザデータ領域の構成と、コンテンツを暗号してユーザデータ領域に記録する光ディスク記録装置の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。この第１０の実施形態は、第６の実施形態において光ディスク記録装置の構成を追加したことを特徴としており、この構成について詳細に説明する。

【０２４０】光ディスク記録装置においては、暗号の結果が一定とならないように暗号の強度を高めるために、入力される暗号鍵を、コンテンツ中の情報である復号鍵変換データを用いて鍵変換器２１１９により、例えば乗算や除算、所定の重み係数を用いた演算などの所定の鍵変換の演算を行ってコンテンツ復号鍵を得た後、当該コンテンツ復号鍵を用いてコンテンツのデータを暗号化する。

【０２４１】すなわち、コンテンツの記録時には、コンテンツのデータと、コンテンツのデータを暗号化するための暗号鍵が光ディスク記録装置に入力される。ここで、コンテンツのデータは鍵変換器２１１９と暗号器２１２０に入力され、暗号鍵は鍵暗号器２１１８と鍵変換器２１１９に入力される。鍵変換器２１１９は、上記入力された暗号鍵に対して、コンテンツ中の一部の情報である第１と第２の復号鍵変換データ２１１５，２１１６を用いて所定の鍵変換の演算を行うことにより、コンテンツ復号鍵を生成して暗号器２１２０に出力する。次いで、暗号器２１２０は、上記入力されるコンテンツのデータを、上記コンテンツ復号鍵を用いて暗号化して暗号化コンテンツを光ディスクのユーザデータ領域２１５０内のＡＶデータ記録セクタ２１５２に記録する。

【０２４２】ここで、光ディスク再生装置において用いる復号鍵変換データとしては、セクタ単位でおおむね異なるようなＡＶデータ中の情報である第２の復号鍵変換データ２１１６や、制御情報が記録されたセクタ中に含まれるコピー世代管理情報やアナログのマクロビジョン

制御フラグなどを含むコピー制御情報である第１の復号鍵変換データ２１１５を利用する。前者の第２の復号鍵変換データを利用することにより、コンテンツのデータを暗号化するためのコンテンツ復号鍵をセクタ毎で、第２の復号鍵変換データの内容に応じて鍵変換器２１１３により復元することが可能となる。また、後者の第１の復号鍵変換データは、その改ざん時にデータの不正利用を容易に検出できるデータであるので、当該第１の復号鍵変換データが改ざんされたときに、コンテンツのデータを復号することができなくすることが容易にできるという効果が得られる。具体的には、ＡＶデータの再生制御に用いられる再生制御情報が記録される再生制御記録セクタのデータを第１の復号鍵変換データとして用いて暗号鍵を所定の変換演算により復号鍵に変換し、これを暗号器２１２０においてコンテンツ復号鍵として用いる。さらには、再生制御記録セクタのデータである第１の復号鍵変換データと、暗号化されたコンテンツが記録されるセクタの非暗号化コンテンツの一部である第２の復号鍵変換データとを含む２つの復号鍵変換データを用いて、暗号鍵を所定の変換演算をすることにより、別のコンテンツ復号鍵を演算し、この別のコンテンツ復号鍵を暗号器２１２０においてコンテンツ復号鍵として用いてもよい。

【０２４３】一方、鍵暗号器２１１８は、上記入力される暗号鍵を、光ディスク再生装置と同様に入力されるディスク鍵を用いて暗号化することにより、暗号化復号鍵を生成する。この暗号化復号鍵のサイズに比較して、セクタヘッダ領域中の復号鍵領域２１０６，２１０９が小さいため、データ分割器２１２１は暗号化復号鍵を複数の分割復号鍵に分割した後、各分割復号鍵を異なる復号鍵領域２１０６，２１０９に記録する。図３７の例では、暗号化復号鍵は２つの暗号化分割復号鍵に分割され、それぞれ連続する２つのセクタの復号鍵領域２１０６，２１０９に記録される。ここでは、鍵暗号器２１１８により暗号鍵である復号鍵に対して暗号化を施しているので、暗号鍵に対する暗号の強度を高めることができる。

【０２４４】コンテンツの再生時には、鍵変換器２１１３は、上述の第１の復号鍵変換データ２１１５と第２の復号鍵変換データ２１１６の情報を用いて、鍵復号器２１１２からの復号鍵を所定の鍵変換の演算を行うことにより、コンテンツ復号鍵を生成して復号器２１１４に出力する。次いで、復号器２１１４は、このコンテンツ復号鍵を用いて、暗号化コンテンツのデータを復号することにより、復号化コンテンツを得る。ここで、鍵変換器２１１３は、第１の復号鍵変換データ２１１５のみの情報を用いて、鍵復号器２１１２からの復号鍵を所定の鍵変換の演算を行ってもよい。

【０２４５】＜第１１の実施形態＞図３８は、本発明に係る第１１の実施形態である光ディスク内のユーザデータ領域の構成と、コンテンツを暗号してユーザデータ領域に記録する光ディスク記録装置の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。この第１１の実施形態は、第７の実施形態において光ディスク記録装置の構成を追加したことを特徴としており、この構成について詳細に説明する。

【０２４６】図３８において、光ディスク記録装置は、図３７の第１０の実施形態と同様に、所定のディスク鍵を用いて暗号鍵の暗号化を行う鍵暗号器２１１８と、コンテンツ中の第１と第２の復号鍵変換データ２１１５，２１１６を用いて暗号鍵に対して所定の鍵変換の演算を行ってコンテンツ復号鍵を演算する鍵変換器２１１９と、上記コンテンツ復号鍵を用いてコンテンツを暗号化する暗号器２１２０を備えて構成される。ここで、鍵暗号器２１１８から出力される復号鍵はリードイン領域２４０１内のメインデータ領域２１０２に記録される。一方、光ディスク再生装置は、図２９の第７の実施形態と同様に、鍵復号器２１１２と、鍵変換器２１１３と、復号器２１１４とを備えて構成される。ここで、リードイン領域２４０１内のメインデータ領域２１０２に記録された復号鍵が読み出されて鍵復号器２１１２に入力され、鍵復号器２１１２は、所定のディスク鍵を用いて復号鍵を復号して鍵変換器２１１３に出力する。また、鍵変換器２１１３は、第１と第２の復号鍵変換データ２１１５，２１１６を用いて、鍵復号器２１１２からの復号鍵に対して所定の鍵変換の演算を行ってコンテンツ復号鍵を演算して復号器２１１４に出力する。

【０２４７】＜第６乃至第９の実施形態の効果＞以上詳述したように、本実施形態に係る記録型光ディスクは、復号鍵をセクタヘッダ領域に配置された所定サイズの復号鍵領域に分割して記録し、あるいは可変長の復号鍵をセクタヘッダ領域に配置された鍵インデックス領域で示された復号鍵領域に記録することによって、セクタヘッダ領域に予め規定されたサイズの復号鍵領域にとらわれることなく、自由な長さの復号鍵を利用できる記録型光ディスクを提供できる。これにより、記録するコンテンツに対する著作権保護レベルに応じて、任意の鍵長を用いた暗号を利用可能とすることができる。

【０２４８】＜好ましい変形例＞以上の実施形態において、上記ディスク識別情報は、好ましくは、書き換えることができないプリピットにより構成され、上記ディスク識別情報には、好ましくは、ディスクが使用される地域を表す地域識別子を有する。また、上記ディスク識別情報には、好ましくは、光ディスク上で記録及び再生可能なコンテンツの種類を示すデータカテゴリ識別子を有する。さらに、上記ディスク識別情報は、好ましくは、秘密鍵を用いて暗号化されてディスク識別情報領域に製造時に記録される。またさらに、上記ディスク識別情報は、好ましくは、データ記録再生領域に記録可能なデー

タの種別、又はデータ記録再生領域から再生可能なデータの種別を表すデータを含む。

【０２４９】以上の実施形態において、好ましくは、コンテンツのデータが記録されるセクタ領域と、デスクランブルキーとの対応関係を管理するデスクランブル領域管理テーブルを有する。また、キー管理情報領域は、好ましくは、ディスク識別情報を鍵として暗号化されたデスクランブルキーを記録するデスクランブルキー領域と、デスクランブルキーの記録状態を表すデスクランブルキーステータス領域を有するキー情報領域と、ディスク上に記録されたコンテンツ再生時に使用するキー情報を記録するコンテンツ情報領域と、コンテンツを再生するために必要なデスクランブルキーを参照するためのポインタを記録したキーインデックス領域とを含む。さらに、コンテンツのデータが記録されるセクタには、好ましくは、上記コンテンツのデータとともに、デスクランブルキーが記録される領域を示すポインタを記録する。

【０２５０】以上の実施形態において、光ディスク記録再生装置のディスク識別情報の再生回路は、好ましくは、秘密鍵を用いて暗号化されたディスク識別情報を解読する回路を備える。また、光ディスク記録再生装置において、ディスク識別情報を鍵として暗号化されるデータは、好ましくは、画像データや音楽データなどのコンテンツのデータである。さらに、ディスク識別情報は、好ましくは、データ記録再生領域に記録可能なデータの種別を表し、ディスク識別情報の再生回路は、上記データの種別により記録可能なコンテンツのデータであるか否かを判断する。またさらに、ディスク識別情報を鍵として用いて復号されるデータは、好ましくは、画像データや音楽データなどのコンテンツのデータである。また、ディスク識別情報は、好ましくは、データ記録再生領域から再生可能なデータの種別を表し、ディスク識別情報の再生回路は、上記データの種別により再生可能なコンテンツのデータであるか否かを判断する。

【０２５１】以上の実施形態において、コンテンツの記録回路は、好ましくは、暗号化された画像データや音楽データなどのコンテンツのデータと、上記コンテンツのデータに施された暗号を解くデスクランブルキーを同一のセクタに記録する。また、コンテンツの再生回路は、好ましくは、暗号化された画像データや音楽データなどのコンテンツのデータと、上記コンテンツのデータに施された暗号を解くデスクランブルキーを同一のセクタから再生する。

【０２５２】以上の実施形態において、キー領域の割当回路又は方法は、好ましくは、デスクランブルキーの記録状態を表すデスクランブルキーステータス領域に領域予約済みフラグを配置し、コンテンツのデータの再生時に使用するキーに関する情報を記録し、コンテンツのデータに対して割り当てたデスクランブルキーの記録領域を表すキーインデックスを記録する。また、デスクランブルキーの配置回路又は方法は、好ましくは、コンテンツ情報領域からコンテンツで使用されるデスクランブルキー領域のインデックスを再生し、記録するデスクランブルキーに対応するキーインデックスに示されるデスクランブルキー領域にデスクランブルキーを配置し、記録するデスクランブルキーに対応するキーインデックスに示されるデスクランブルキーステータス領域に記録済みフラグを配置する。

【０２５３】以上の実施形態において、光ディスク再生装置は、好ましくは、ディスク識別情報を再生し、コンテンツが再生可能であるか否かを調べ、キー管理情報を再生し、画像データや音楽データなどのコンテンツのデータが記録されたセクタを再生し、再生されたセクタからデスクランブルキーを取得する。さらに、好ましくは、再生したコンテンツのデータをデスクランブルキーによりデスクランブルし出力する。

【０２５４】以上の実施形態において、コンテンツのデータを記録する方法は、好ましくは、第１のディスク情報が記録されている第１の情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２の情報領域と、光ビームを照射することにより情報の記録が可能なユーザデータ領域とを有する光ディスクの上記ユーザデータ領域にコンテンツを記録する際に、少なくとも上記第２のディスク情報を用いた演算により復号して再生することができるように、暗号化して記録する。ここで、好ましくは、ユーザデータ領域内に、暗号化されて記録されたデータを解読するための鍵情報を記録する鍵情報記録領域を有する。

【０２５５】以上の実施形態において、コンテンツのデータを記録する方法は、好ましくは、第１のディスク情報が記録されている第１の情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２の情報領域と、光ビームを照射することにより情報の記録が可能なユーザデータ領域と、上記ユーザデータ領域内に、暗号化されて記録されたコンテンツを解読するための鍵情報を記録する鍵情報記録領域とを有する光ディスクの、上記ユーザデータ領域にコンテンツを記録する際に、少なくとも上記第２のディスク情報と、上記鍵情報を用いた演算により復号して再生することができるように、暗号化して記録する。

【０２５６】以上の実施形態において、連続する複数のセクタに、分割された複数の分割復号鍵を記録する復号鍵領域を有する光ディスクのセクタにおいて、好ましくは、ＡＶデータを含むデータのサイズが（メインデータサイズ）×（復号鍵の分割数）に満たないメインデータ領域に、ダミーデータを記録する。また、ＥＣＣブロックにおいて、好ましくは、連続する複数のセクタに分割された分割復号鍵を記録した復号鍵領域を有するセクタが、（ＥＣＣブロック単位）／（復号鍵の分割数）回だけ記録され、ＡＶデータを含むデータのサイズが（メイ

ンデータサイズ）×（ＥＣＣブロック単位）に満たないメインデータ領域に、ダミーデータを記録する。

【０２５７】以上の実施形態において、ＡＶデータを含むデータに施された暗号を復号するための復号鍵は、好ましくは、所定のサイズを有する複数の分割復号鍵に分割され、分割された複数の分割復号鍵は、復号鍵テーブルの連続する複数の復号鍵領域に記録される。また、上記復号鍵テーブルは、好ましくは、書き換え可能なリードイン領域内のメインデータ領域に記録される。さらに、復号鍵テーブルの記録状態を表す情報は、好ましくは、復号鍵テーブルの各復号鍵領域に固定値として記録される。またさらに、復号鍵テーブルは、光ディスクの内周と外周に配置された異なる上記ＥＣＣブロックに複数回だけ記録される。

【０２５８】以上の実施形態において、データ暗号化装置であるエンコード装置３１０１と、光ディスク記録再生装置である光ディスク装置３１０２は、好ましくは、相互認証方式によりバス鍵の共有を行う。また、データ復号化装置であるデコード装置３１０３と光ディスク記録再生装置である光ディスク装置３１０２は、好ましくは、相互認証方式によりバス鍵の共有を行う。

【０２５９】以上の実施形態においては、ＲＡＭ型を含む書き換え型又は追記型の光ディスクであるデータを記録することができる記録型光ディスクについて説明しているが、本発明はこれに限らず、予め記録されたデータを読み出して再生することができるが新たに記録することができない再生専用型光ディスクに適用できる。再生専用型光ディスクの場合においては、データ記録再生領域をデータを読み出して再生するデータ再生領域と置き換え、コンテンツのデータやその他の種々の制御情報のデータは製造時に予め記録される。ここで、記録型光ディスクは、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＭＯ、ＭＤ、ＤＶＤ－ＲＡＭなどを含む。再生専用型光ディスクは、音楽ＣＤ、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭなどを含む。

【０２６０】

【発明の効果】以上詳述したように、本発明に係る光ディスクによれば、ユーザデータ領域への記録動作や再生動作を光ディスク毎に行うディスク識別情報が書き換え不可能な再生専用領域に記録されることにより、利用者による光ディスク上へのコンテンツの記録動作や再生動作を光ディスクの製造時に記録する情報を用いて制御することができる。

【０２６１】また、本発明に係る光ディスクによれば、書き換えが不可能な再生専用のディスク識別情報を鍵として暗号化されたデータが光ディスク上のユーザデータ領域に記録することにより、利用者によるユーザデータ領域の他の記録型光ディスクにコピーしたとしても、ディスク識別情報をコピーすることができず、データの正しい復号並びに再生が不可能とすることができる。

【０２６２】さらに、本発明に係る光ディスクによれば、暗号化されたデータと暗号を解くデスクランブルキーとが異なるセクタ領域に記録されることにより、映画や音楽などの著作権保護が必要なデータの取得と暗号を解くためのデスクランブルキーの取得を独立に行うことが可能となる。さらに、ディスク識別情報を鍵としてデスクランブルキーを暗号化して記録することにより、利用者によるユーザデータ領域の他の記録型光ディスクにコピーしたとしても、ディスク識別情報をコピーすることができず、データの正しい復号並びに再生が不可能とし、コピー先の光ディスクのディスク識別情報を鍵として暗号化したデスクランブルキーを取得し記録することで、データの正しい復号並びに再生を可能とすることができる。

【０２６３】また、本発明に係る光ディスクによれば、第１のディスク情報が記録されている第１の情報領域と、個々のディスクを識別するための第２のディスク情報が記録されている第２の情報領域と、光ビームを照射することにより情報の記録が可能なユーザデータ領域を有する。従って、従来技術の光ディスクに、上記光ディスクを識別する情報を付加することにより、光ディスクの管理を容易に実現することができる。ここで、上記第２の情報領域は、好ましくは、上記第１の情報領域内に記録されているものであり、上記第１の情報領域を再生する光ピックアップによって再生することができる。また、上記第２の情報領域は、上記第１の情報領域内の記録膜を、半径方向に長い形状でかつ複数個のトリミング領域が形成されるように、部分的に除去することにより記録されているものであり、容易に上記第２のディスク情報が改ざんされることを防止することができる。

【０２６４】さらに、本発明に係る光ディスクによれば、復号鍵をセクタヘッダ領域に配置された所定サイズの復号鍵領域に分割して記録し、あるいは可変長の復号鍵をセクタヘッダ領域に配置された鍵インデックス領域で示された復号鍵領域に記録することによって、セクタヘッダ領域に予め規定されたサイズの復号鍵領域にとらわれることなく、自由な長さの復号鍵を利用できる記録型光ディスクを提供できる。これにより、記録するコンテンツに対する著作権保護レベルに応じて、任意の鍵長を用いた暗号を利用可能とすることができる。

【図面の簡単な説明】

【図１】　本発明に係る第１の実施形態である記録型光ディスク１００のデータ記録領域を示す平面図である。

【図２】　（ａ）は図１の光ディスク１００のＢＣＡ１０６を形成するときの装置構成を示すブロック図及び縦断面図であり、（ｂ）は図１の光ディスク１００のＢＣＡ１０６を形成した後の光ディスク１００の縦断面図及びその水平方向に対する反射光の強度を示すグラフである。

【図３】　図１のＢＣＡ１０６の記録フォーマットを示す図である。

【図４】　図１のユーザデータ領域１０２内のセクタデータ４０１のセクタ構造を示す図である。
【図５】　図１のキー管理情報領域１０７の構成を示す図である。
【図６】　（ａ）は第１の実施形態の変形例に係る、図１のセクタデータ４０１にデスクランブルキー及びＡＶデータを記録する記録方法を示すブロック図であり、（ｂ）は第１の実施形態に係る、図１のセクタデータ４０１にデスクランブルキーへのキーインデックス及びＡＶデータを記録する記録方法を示すブロック図である。
【図７】　本発明に係る第２の実施形態である光ディスク記録再生装置の構成を示すブロック図である。
【図８】　図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるＡＶデータの記録処理を示すフローチャートである。
【図９】　図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるキー管理情報領域の割り当て処理を示すフローチャートである。
【図１０】　図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるデスクランブルキーの記録処理を示すフローチャートである。
【図１１】　図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるＡＶデータの再生処理を示すフローチャートである。
【図１２】　図７の光ディスク記録再生装置の制御ＣＰＵ７１０によって実行されるデスクランブルキーの取得処理を示すフローチャートである。
【図１３】　第１の実施形態の変形例に係る、暗号化デスクランブルキーから正規のデスクランブルキーであるか否かを判定するための方法を示すブロック図である。
【図１４】　第１の実施形態の変形例に係る、デスクランブル領域管理テーブルの構成を示す図である。
【図１５】　（ａ）は第１の実施形態においてコンテンツの記録時に地域識別子を記録する場合に、同一の地域内で、並びに異なる地域で、コンテンツのコピーや再生が可能であるか否かを示す図であり、（ｂ）は第１の実施形態において地域識別子が光ディスクの出荷時に予め記録されている場合に、同一の地域内で、並びに異なる地域で、コンテンツのコピーや再生が可能であるか否かを示す図である。
【図１６】　本発明に係る第３の実施形態である光ディスク１１０１のデータ記録領域を示す平面図である。
【図１７】　第３の実施形態に係るＢＣＡ再生回路１４０１における再生信号１２０１及び再生２値化信号１２０７の信号波形を示す波形図である。
【図１８】　第３の実施形態に係るＢＣＡ再生回路１４０１の構成を示すブロック図である。
【図１９】　第３の実施形態に係る光ディスク記録再生システムの構成を示すブロック図である。
【図２０】　本発明に係る第４の実施形態である光ディスク記録再生システムの構成を示すブロック図である。
【図２１】　本発明に係る第５の実施形態である光ディスク１６０１のデータ記録領域を示す平面図である。
【図２２】　第５の実施形態に係る光ディスク記録再生システムの構成を示すブロック図である。
【図２３】　第５の実施形態に係るＩＤ付与テーブルの構成を示す表である。
【図２４】　第３の実施形態の変形例に係る光ディスク１１０１ａのデータ記録領域を示す平面図である。
【図２５】　第５の実施形態の変形例に係る光ディスク１６０１ａのデータ記録領域を示す平面図である。
【図２６】　本発明に係る第６の実施形態である光ディスク内のユーザデータ領域の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。
【図２７】　第６の実施形態に係る光ディスクにおいて、ユーザデータ領域への著作権制御情報と復号鍵の配置と、メインデータ領域への暗号化コンテンツの配置を示すブロック図である。
【図２８】　第６の実施形態に係る光ディスクにおいて、エラー訂正の単位が複数のセクタにまたがる場合の配置を示すブロック図である。
【図２９】　本発明に係る第７の実施形態である光ディスク内のリードイン領域２４０１とユーザデータ領域２４０２の構成と、リードイン領域２４０１とユーザデータ領域２４０２のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。
【図３０】　（ａ）は第７の実施形態に係る光ディスク内のリードイン領域のメインデータ領域において、復号鍵の初期値で未記録状態を表示する場合のデータ構成を示すブロック図であり、（ｂ）は第７の実施形態に係る光ディスク内のリードイン領域のメインデータ領域において、復号鍵状態テーブルで記録状態を表示する場合のデータ構成を示すブロック図である。
【図３１】　第７の実施形態に係る光ディスクにおいて復号鍵の配置を示すブロック図である。
【図３２】　本発明に係る第８の実施形態である光ディスクのデータをファイル管理システムにより管理するときのデータ構成を示すブロック図である。
【図３３】　第８の実施形態に係るファイル管理システムによって実行される、著作権保護を必要とするコンテンツの記録処理を示すフローチャートである。
【図３４】　第８の実施形態に係るファイル管理システムによって実行される、コンテンツの再生処理を示すフローチャートである。
【図３５】　第８の実施形態に係るファイル管理システムによって実行される、コンテンツの削除処理を示すフローチャートである。
【図３６】　本発明に係る第９の実施形態である光ディスクシステムの構成を示すブロック図である。

【図３７】　本発明に係る第１０の実施形態である光ディスク内のユーザデータ領域の構成と、コンテンツを暗号してユーザデータ領域に記録する光ディスク記録装置の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。

【図３８】　本発明に係る第１１の実施形態である光ディスク内のユーザデータ領域の構成と、コンテンツを暗号してユーザデータ領域に記録する光ディスク記録装置の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。

【図３９】　従来技術のＤＶＤ－ＲＯＭのユーザデータ領域の構成と、ユーザデータ領域のデータから暗号化コンテンツを復号する光ディスク再生装置の構成を示すブロック図である。

【符号の説明】

１００…光ディスク、
１０１…リードイン領域、
１０２…ユーザデータ領域、
１０３…リードアウト領域、
１０４…再生専用領域、
１０５…記録再生領域、
１０６…バーストカッティング領域（ＢＣＡ）、
１０７…キー管理情報領域、
２０１…基板、
２０２…記録層、
２０３…反射層、
２０４…接着層、
２０５…反射層、
２０６…記録層、
２０７…基板、
２１１…高パワーレーザ光源、
２１２…フォーカスレンズ、
３０１…同期コード、
３０２…誤り検出コード、
３０３…誤り訂正コード、
３０４…ＢＣＡデータ、
３０５…ディスク識別情報、
４０１…セクタデータ、
４０２…ヘッダ、
４０３…メインデータ、
４０４…エラー検出コード、
４０５…データＩＤ、
４０６…ＩＤエラー検出コード、
４０７…スクランブル制御情報、
４０８，４０８ａ…キー情報、
５０１…キー情報領域、
５０２…コンテンツ情報領域、
５０３…キーインデックスリスト領域、
５０４…記録済みキー数、
５０５…デスクランブルキー領域、
５０６…キーステータス領域、
５０７…コンテンツ数、
５０８…コンテンツ情報、
５０９…キーインデックス、
７０１…記録型光ディスク、
７０２…光学ヘッド、
７０３…記録再生制御回路、
７０４…変復調回路、
７０５…誤り検出及び訂正回路、
７０６…バッファメモリ、
７０７…デスクランブル回路、
７０８…ＭＰＥＧ復号回路、
７０９…出力回路、
７１０…制御ＣＰＵ、
７１１…通信回路、
７１２…データ受信回路、
８０１…暗号化デスクランブルキー、
８０２…デスクランブルキー、
８０３…誤り検出コード、
１１０１，１１０１ａ…光ディスク、
１１０２…コントロールユーザデータ領域、
１１０３…ユーザデータ領域、
１１０４，１１０４ａ…ＢＣＡ、
１１０５，１１０５ａ…トリミング領域、
１２０１…再生信号、
１２０２乃至１２０４…トリミング部分、
１２０５，１２０６…スライスレベル、
１２０７…再生２値化信号、
１３０１…光ピックアップ、
１３０２…プリアンプ、
１３０３…低域通過フィルタ（ＬＰＦ）、
１３０４…２値化回路、
１３０５…復調回路、
１３０６…ディスクＩＤ信号、
１４０１…ＢＣＡ再生回路
１４０２…ディスクＩＤ信号、
１４０３，１４０４…インターフェース、
１４０５…ネットワーク、
１４０６…暗号化部、
１４０７…コンテンツメモリ、
１４０８…暗号化エンコーダ、
１４０９…暗号化コンテンツ、
１４１０…光ディスク記録再生装置、
１４１１…記録回路、
１４１２…データ再生部、
１４１３…暗号デコーダ、
１４１４…出力信号、
１５０１…ＣＡＴＶ会社装置、

１５０２…コンテンツメモリ、
１５０３…第１暗号鍵メモリ、
１５０４…第１暗号化エンコーダ、
１５０５…第１暗号化コンテンツ、
１５０６…ＣＡＴＶデコーダ、
１５０７…鍵発行センター装置、
１５０７ａ…制御部、
１５０８…システムＩＤメモリ、
１５０９…入力されたタイトルコード、
１５１０…時間制限情報メモリ、
１５１１…記録許可コードメモリ、
１５１２…鍵（Ｋ）、
１５１３…第１暗号デコーダ、
１５１４…光ディスク記録再生装置、
１５１５…ディスクＩＤ信号、
１５１６…第２暗号化エンコーダ、
１５１７…第２暗号化コンテンツ、
１５１８…記録回路、
１５１９…データ再生部、
１５２０…第２暗号デコーダ、
１５２１…ＢＣＡ再生回路、
１５２２…ＩＣカード、
１５２３…会社識別信号メモリ、
１５２４…ＩＣカード、
１５２５…出力信号、
１５２６…会社識別信号メモリ、
１５２７…クロック回路、
１５３０…テレビジョン装置、
１６０１，１６０１ａ…光ディスク、
１６０２…コントロールユーザデータ領域、
１６０３…ユーザデータ領域、
１６０４，１６０４ａ…ＢＣＡ、
１６０５…鍵情報記録領域、
１６０６，１６０６ａ…トリミング領域、
１７０１…ＣＡＴＶ会社装置、
１７０２…コンテンツメモリ、
１７０３…第１暗号鍵、
１７０４…第１暗号化エンコーダ、
１７０５…鍵（Ｋ）、
１７０６…ＣＡＴＶデコーダ、
１７０７…鍵発行センター装置、
１７０７ａ…制御部、
１７０８…システムＩＤメモリ、
１７０９…入力されたタイトルコード、
１７１０…時間制限情報メモリ、
１７１２…鍵（Ｋ）、
１７１３…第１暗号化デコーダ、
１７１４…光ディスク記録再生装置、
１７１５…ディスクＩＤ、
１７１６…入力されたタイトルコード、

１７１７…記録回路、
１７１８…鍵（ＤＫ）、
１７１９…鍵情報記録回路、
１７２０…ＢＣＡ再生回路、
１７２１…データ再生部、
１７２２…第２暗号デコーダ、
１７２３…鍵情報再生部、
１７２４…出力信号、
１７２５…クロック回路、
１７３０…テレビジョン装置、
２１０１…セクタヘッダ領域、
２１０２…メインデータ領域、
２１０３…誤り検出コード、
２１０４…セクタアドレス、
２１０５…著作権制御情報、
２１０６…復号鍵領域、
２１０７…非暗号化コンテンツ、
２１０８…暗号化コンテンツ、
２１０９…復号鍵領域、
２１１０…復号鍵変換データ、
２１１１…データ連結器、
２１１２…鍵復号器、
２１１３…鍵変換器、
２１１４…復号器、
２１１５…第１の復号鍵変換データ、
２１１６…第２の復号鍵変換データ、
２１１７…非暗号化制御情報、
２１１８…鍵暗号器、
２１１９…鍵変換器、
２１２０…暗号器、
２１２１…データ分割器、
２１５０…ユーザデータ領域、
２１５１…制御情報記録セクタ、
２１５２…ＡＶデータ記録セクタ、
２２０１…第１の復号鍵領域、
２２０２…第２の復号鍵領域、
２２０３…補完データ、
２２０４…暗号化コンテンツ、
２４０１…リードイン領域、
２４０２…ユーザデータ領域、
２４０３…鍵インデックス領域、
２４０４…復号鍵テーブル、
２４５１…制御情報記録セクタ、
２４５２…ＡＶデータ記録セクタ、
２５０１…未記録状態データ、
２５０２…復号鍵状態テーブル、
２５０３…記録状態データ、
２６０１…リードイン領域、
２６０２…ユーザデータ領域、
２６０３…リードアウト領域、

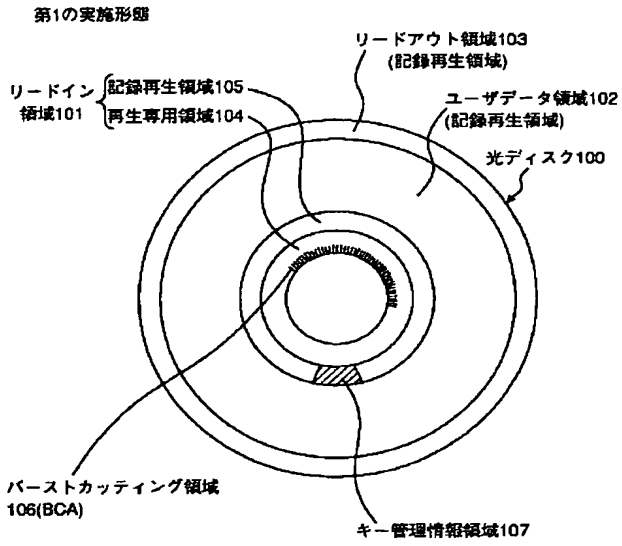
85

２７０１…ファイルエントリ（１）、
２７０２…ファイルエントリ（２）、
２７０３…ファイル（１）、
２７０４…ファイル（２）、
２７０５…ファイル（１）のエクステント（１）、
２７０６…ファイル（２）のエクステント（１）、
２７０７…復号鍵テーブル、
２７０８…鍵インデックス領域、
２７５１…ファイル管理情報領域、
３１０１…エンコード装置、
３１０２…光ディスク装置、
３１０３…デコード装置、
３１０４…パーソナルコンピュータ、
３１１１…復号鍵メモリ、
３１１２…バス暗号回路、
３１１３…復号鍵テーブルメモリ、

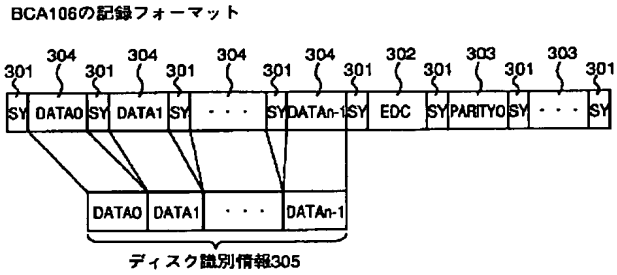
86

＊３１１４…バス暗号及び復号回路、
３１１５…バス暗号化復号鍵テーブルメモリ、
３１１６…復号鍵状態テーブルメモリ、
３１１７…バス復号回路、
３１１８…復号鍵メモリ、
３１１９…記録再生回路、
３１２０，３１２１，３１２３，３１２４…インターフェース、
３１３０…制御部、
３１３１…コンテンツメモリ、
３１３２…符号化回路、
３１３３…暗号鍵メモリ、
３１３４…暗号回路、
３１４１…復号化回路、
３１５１…ＰＣＩバス、
＊　３１５２…ＳＣＳＩバス。

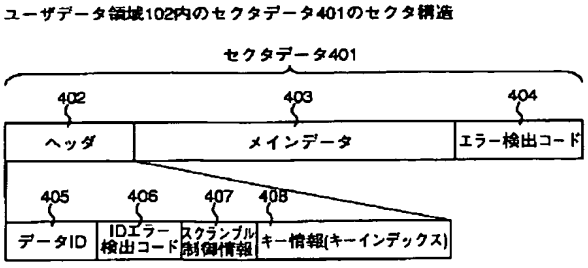
【図１】



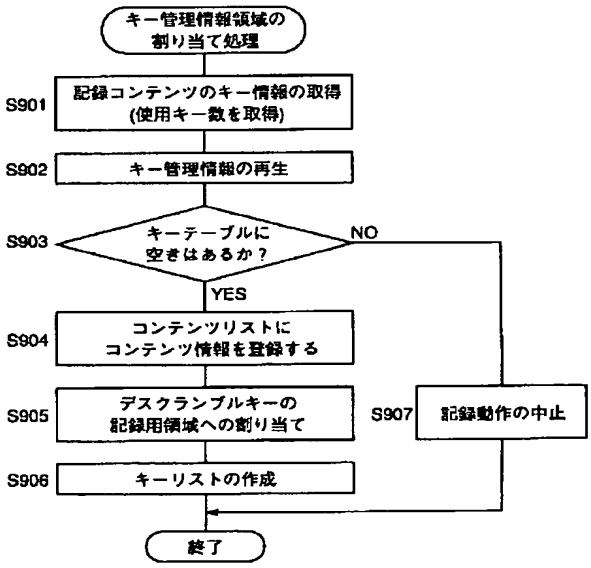
【図３】



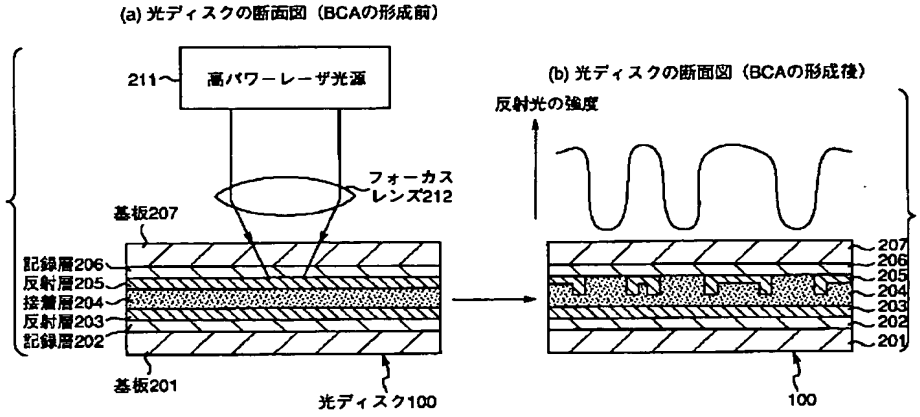
【図４】



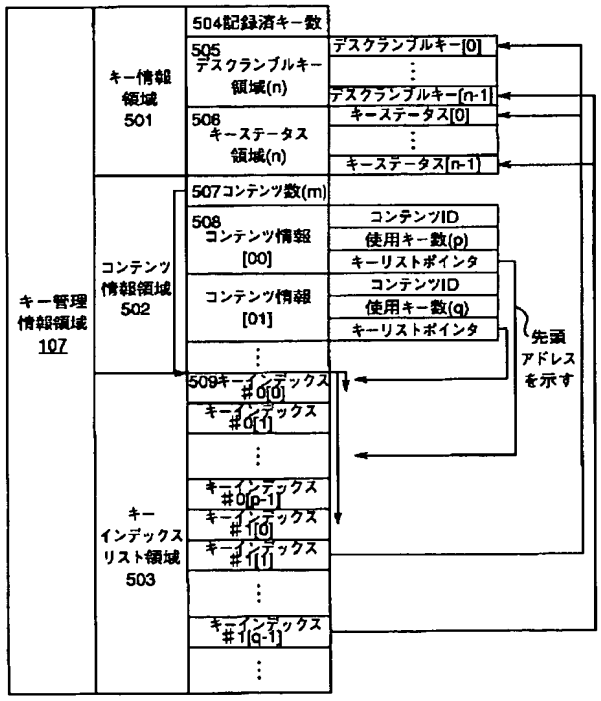
【図９】



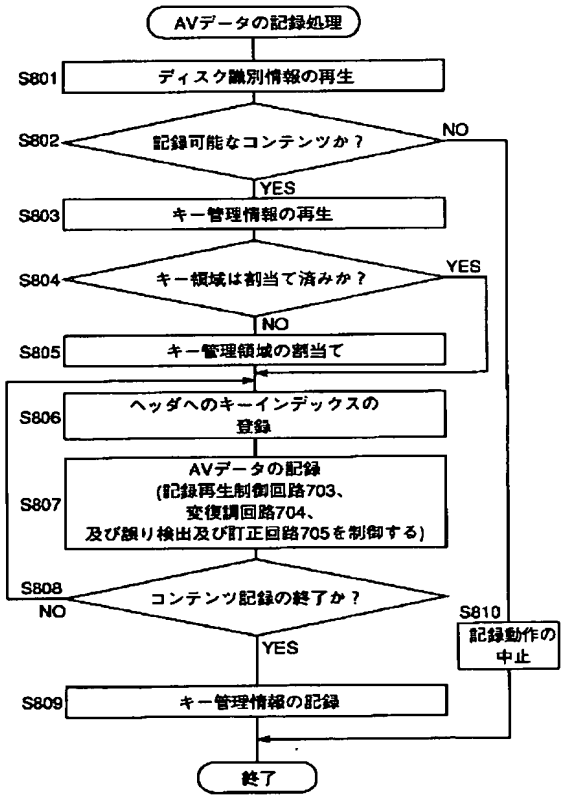
【図２】


(a) 光ディスクの断面図（BCAの形成前）
211
高パワーレーザ光源
フォーカスレンズ212
基板207
記録層206
反射層205
接着層204
反射層203
記録層202
基板201
光ディスク100
(b) 光ディスクの断面図（BCAの形成後）
反射光の強度
207
206
205
204
203
202
201
100

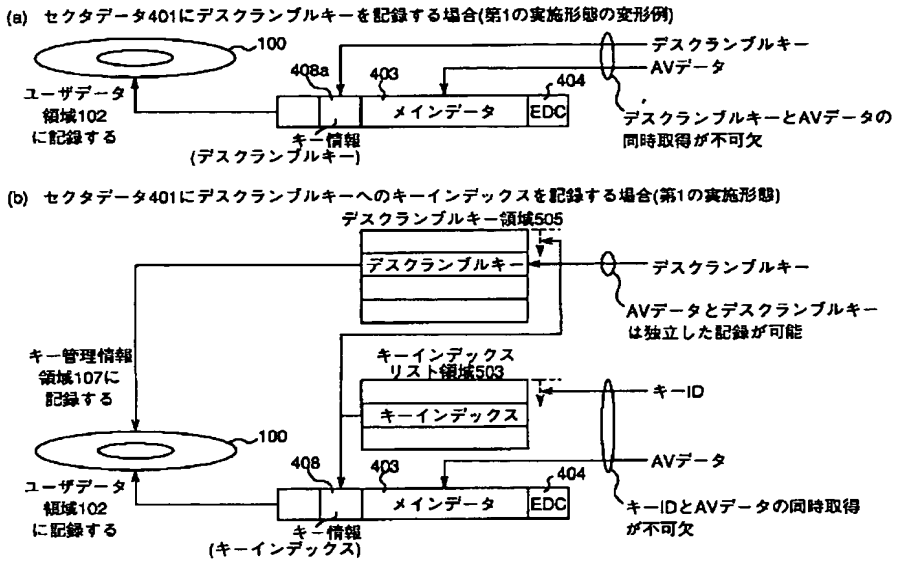
【図５】


キー管理情報領域 107
キー情報領域 501
コンテンツ情報領域 502
キーインデックスリスト領域 503
504記録済キー数
505 デスクランブルキー領域(n)
デスクランブルキー[0]
デスクランブルキー[n-1]
506 キーステータス領域(n)
キーステータス[0]
キーステータス[n-1]
507コンテンツ数(m)
508 コンテンツ情報[00]
コンテンツID
使用キー数(p)
キーリストポインタ
コンテンツ情報[01]
コンテンツID
使用キー数(q)
キーリストポインタ
先頭アドレスを示す
509キーインデックス #0[0]
キーインデックス #0[1]
キーインデックス #0[p-1]
キーインデックス #1[0]
キーインデックス #1[1]
キーインデックス #1[q-1]

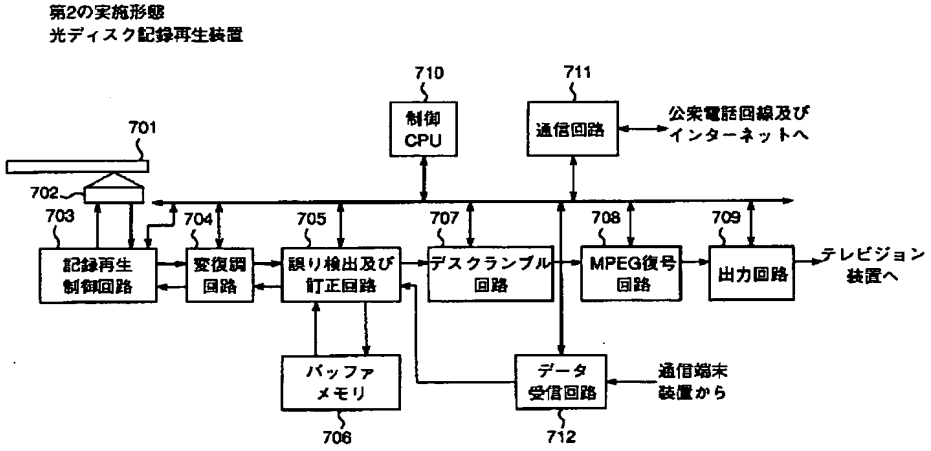
【図８】


AVデータの記録処理
S801
ディスク識別情報の再生
S802
記録可能なコンテンツか？
NO
YES
S803
キー管理情報の再生
S804
キー領域は割当て済みか？
YES
NO
S805
キー管理領域の割当て
S806
ヘッダへのキーインデックスの登録
S807
AVデータの記録
(記録再生制御回路703、変復調回路704、及び誤り検出及び訂正回路705を制御する)
S808
コンテンツ記録の終了か？
NO
YES
S810
記録動作の中止
S809
キー管理情報の記録
終了

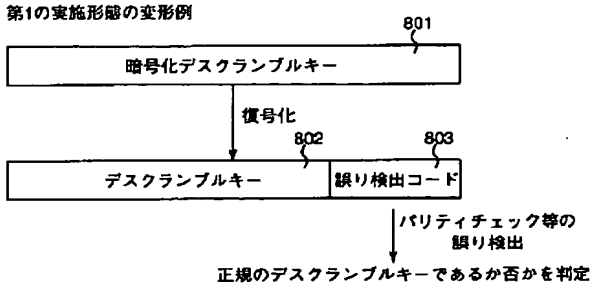
【図６】



【図７】



【図１３】



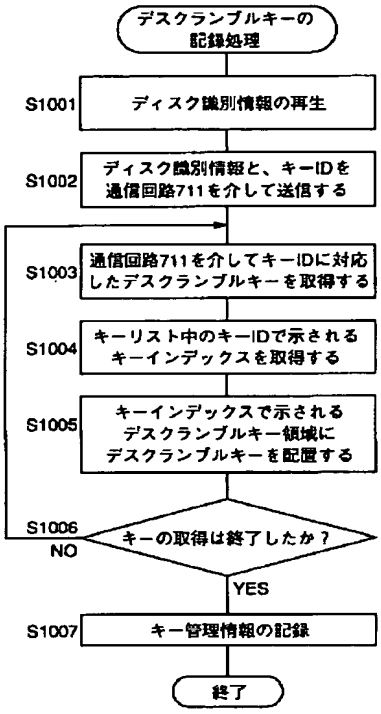
【図１４】

第1の実施形態の変形例

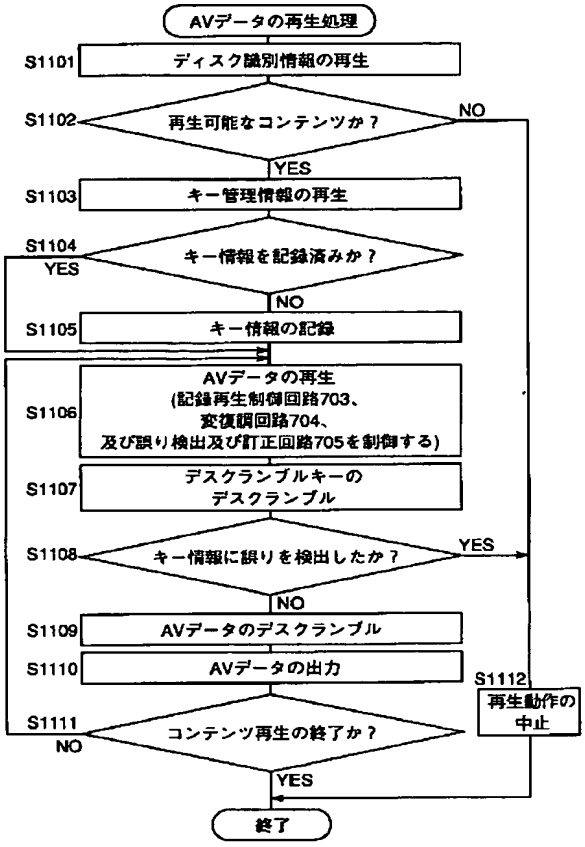
デスクランブル領域管理テーブル

1	開始アドレス1	終了アドレス1	デスクランブルキー1
2	開始アドレス2	終了アドレス2	デスクランブルキー2
⋮	⋮	⋮	⋮
n	開始アドレスn	終了アドレスn	デスクランブルキーn

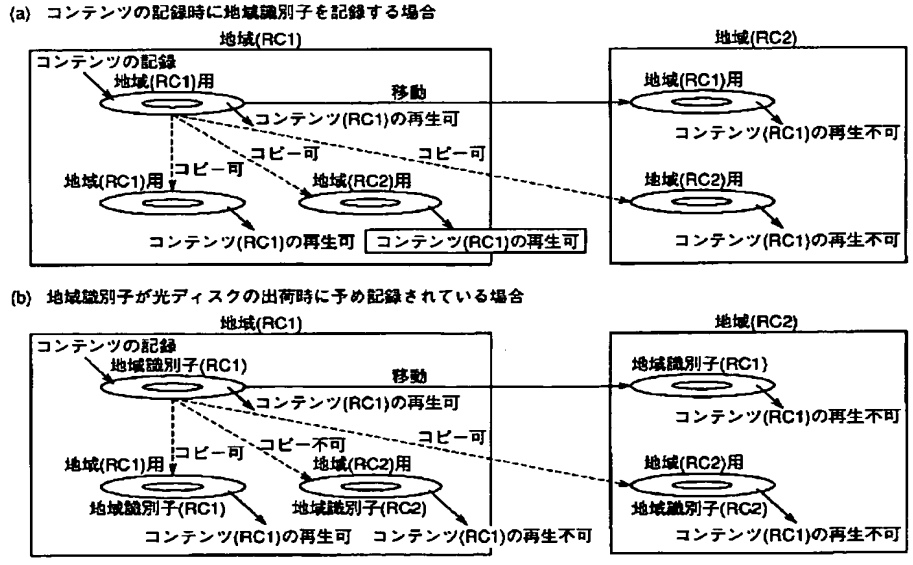
【図１０】


デスクランブルキーの記録処理
S1001
ディスク識別情報の再生
S1002
ディスク識別情報と、キーIDを通信回路711を介して送信する
S1003
通信回路711を介してキーIDに対応したデスクランブルキーを取得する
S1004
キーリスト中のキーIDで示されるキーインデックスを取得する
S1005
キーインデックスで示されるデスクランブルキー領域にデスクランブルキーを配置する
S1006
キーの取得は終了したか？
NO
YES
S1007
キー管理情報の記録
終了

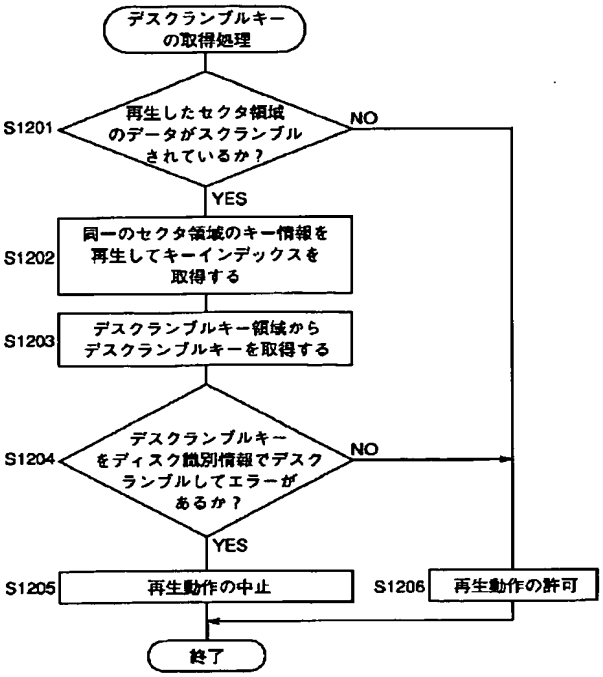
【図１１】


AVデータの再生処理
S1101
ディスク識別情報の再生
S1102
再生可能なコンテンツか？
NO
YES
S1103
キー管理情報の再生
S1104
キー情報を記録済みか？
YES
NO
S1105
キー情報の記録
S1106
AVデータの再生
(記録再生制御回路703、変復調回路704、及び誤り検出及び訂正回路705を制御する)
S1107
デスクランブルキーのデスクランブル
S1108
キー情報に誤りを検出したか？
YES
NO
S1109
AVデータのデスクランブル
S1110
AVデータの出力
S1111
コンテンツ再生の終了か？
NO
YES
S1112
再生動作の中止
終了

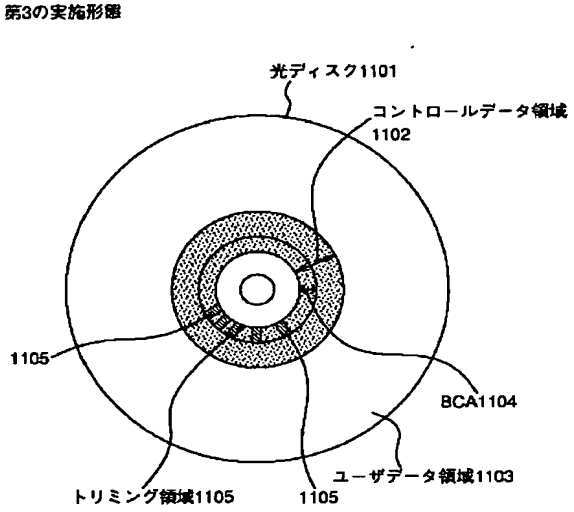
【図１５】


(a) コンテンツの記録時に地域識別子を記録する場合
地域(RC1)
コンテンツの記録
地域(RC1)用
移動
コンテンツ(RC1)の再生可
コピー可
コピー可
コピー可
地域(RC1)用
地域(RC2)用
コンテンツ(RC1)の再生可
コンテンツ(RC1)の再生可
地域(RC2)
地域(RC1)用
コンテンツ(RC1)の再生不可
地域(RC2)用
コンテンツ(RC1)の再生不可
(b) 地域識別子が光ディスクの出荷時に予め記録されている場合
地域(RC1)
コンテンツの記録
地域識別子(RC1)
移動
コンテンツ(RC1)の再生可
コピー可
コピー不可
コピー可
地域(RC1)用
地域(RC2)用
地域識別子(RC1)
地域識別子(RC2)
コンテンツ(RC1)の再生可
コンテンツ(RC1)の再生不可
地域(RC2)
地域識別子(RC1)
コンテンツ(RC1)の再生不可
地域(RC2)用
地域識別子(RC2)
コンテンツ(RC1)の再生不可

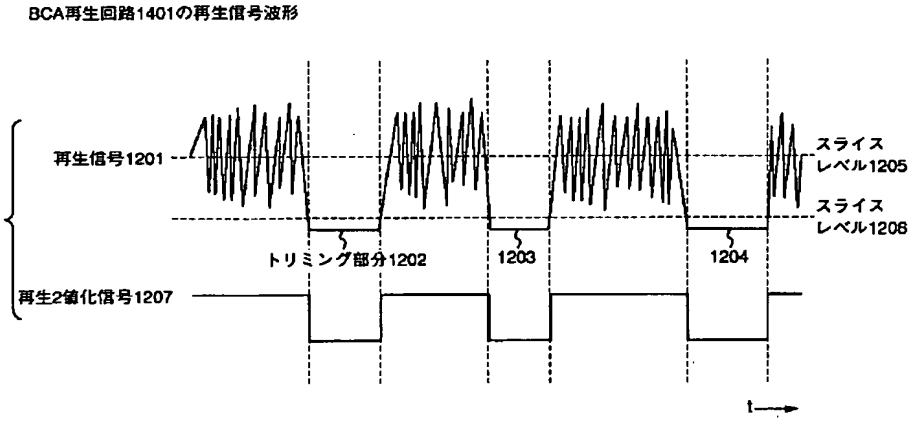
【図１２】



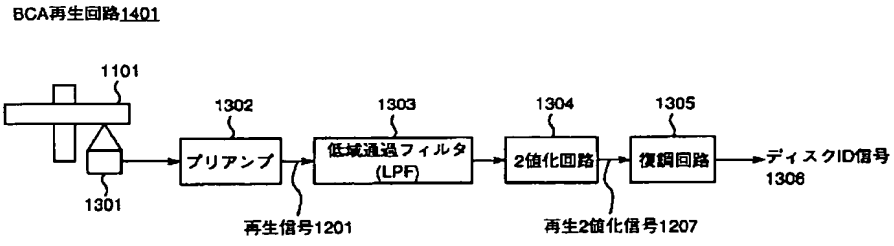
【図１６】



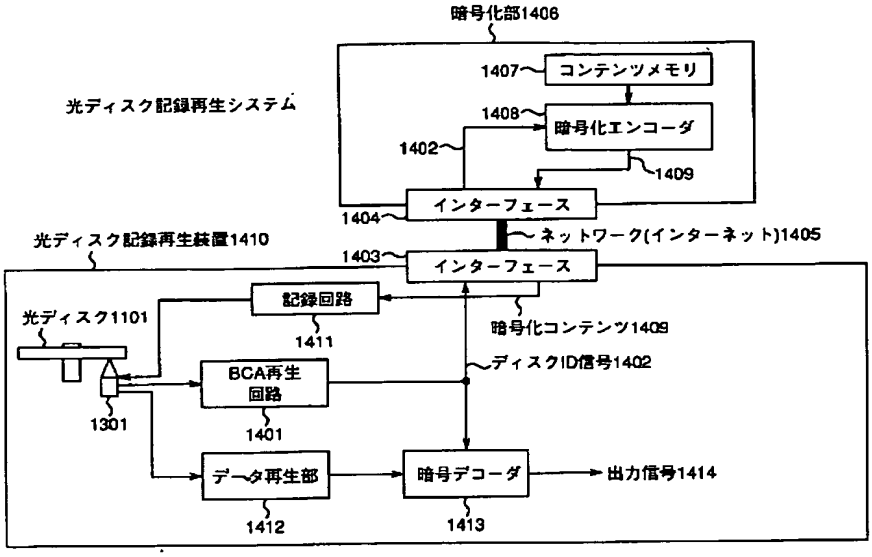
【図１７】



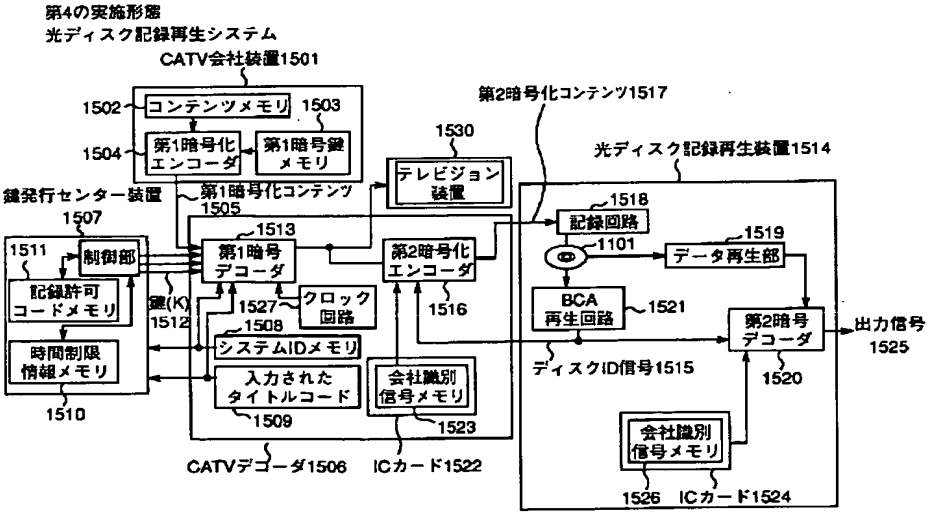
【図１８】



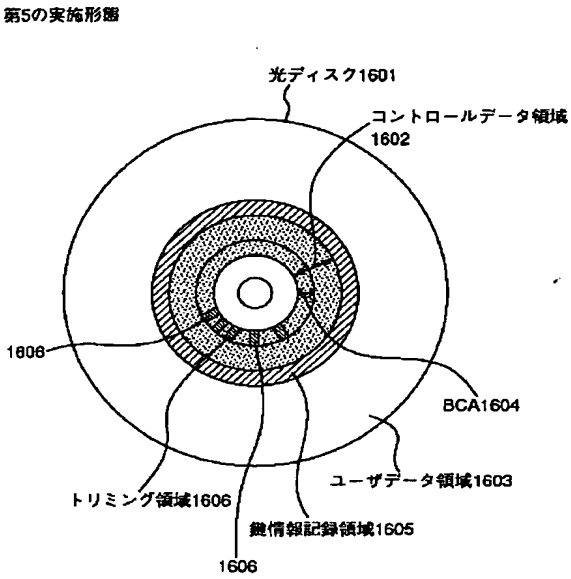
【図１９】


暗号化部1406
1407
コンテンツメモリ
光ディスク記録再生システム
1408
暗号化エンコーダ
1402
1409
インターフェース
1404
ネットワーク(インターネット)1405
光ディスク記録再生装置1410
1403
インターフェース
記録回路
光ディスク1101
1411
暗号化コンテンツ1409
ディスクID信号1402
BCA再生回路
1401
1301
データ再生部
暗号デコーダ
出力信号1414
1412
1413

【図２０】


第4の実施形態
光ディスク記録再生システム
CATV会社装置1501
1502
コンテンツメモリ
1503
1504
第1暗号化エンコーダ
第1暗号鍵メモリ
第1暗号化コンテンツ
1505
第2暗号化コンテンツ1517
1530
テレビジョン装置
光ディスク記録再生装置1514
鍵発行センター装置
1507
1518
記録回路
1513
1519
1511
制御部
第1暗号デコーダ
第2暗号化エンコーダ
1101
データ再生部
記録許可コードメモリ
鍵(K)
1512
1527
クロック回路
1516
BCA再生回路
1521
第2暗号デコーダ
出力信号
1525
1508
システムIDメモリ
ディスクID信号1515
時間制限情報メモリ
入力された タイトルコード
会社識別信号メモリ
1520
1510
1509
1523
会社識別信号メモリ
CATVデコーダ1506
ICカード1522
1526
ICカード1524

【図２１】

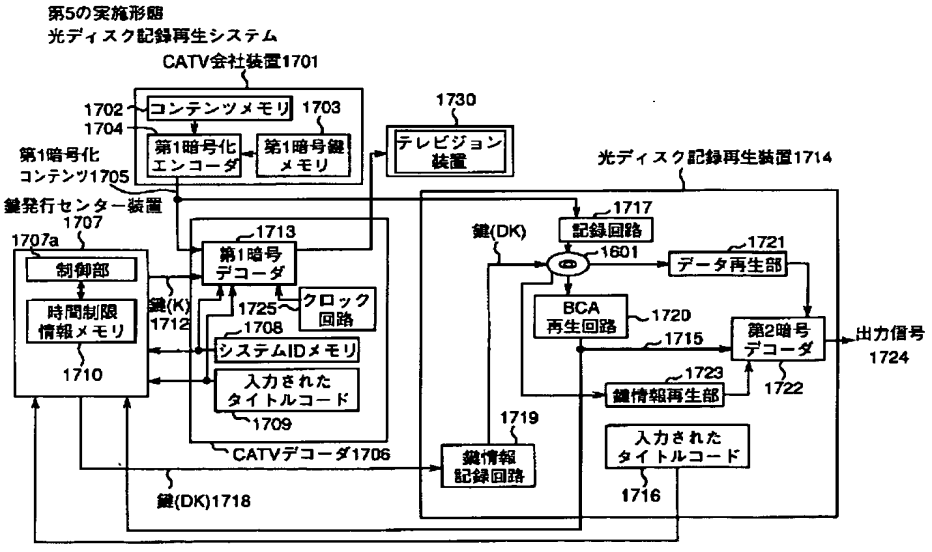


【図２３】

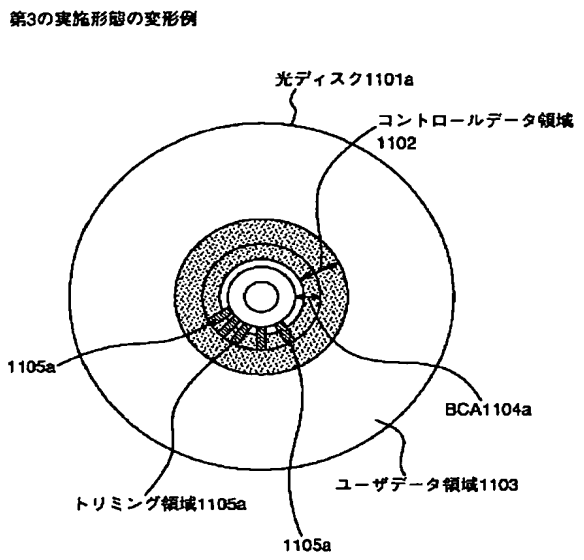
ID付きテーブル

タイトルコードT		T1	T2	T3
第1復号鍵FK		FK1	FK2	FK3
時間制限情報TIME		TIME1	TIME2	TIME3
システムID	DID1	K11	K12	K13
	DID2	K21	K22	K23
	DID3	K23	K32	K33
ディスクID	BCAS1	DK11	DK12	DK13
	BCAS2	DK21	DK22	DK23
	BCAS3	DK31	DK32	DK33

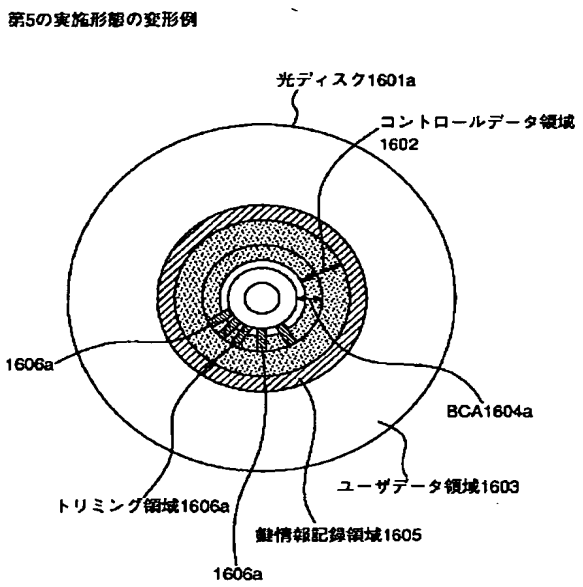
【図２２】



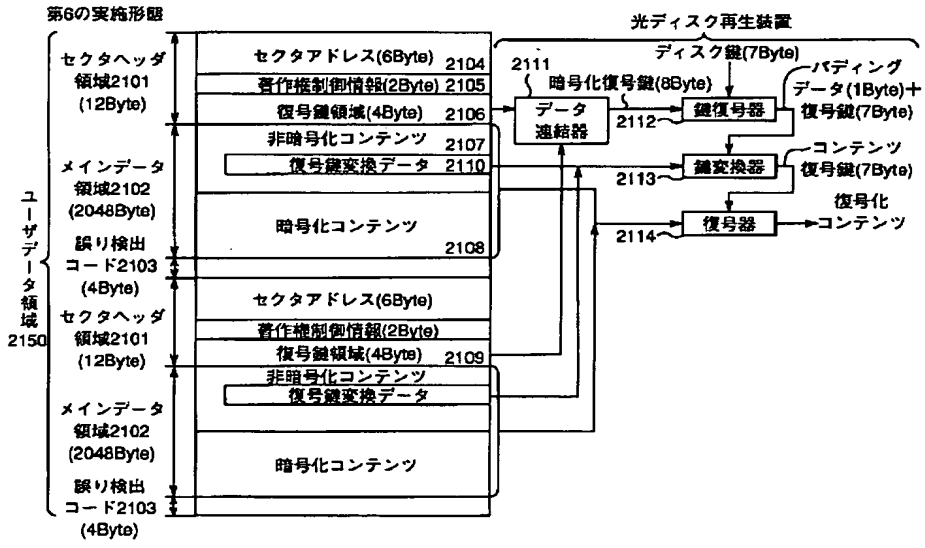
【図２４】


第3の実施形態の変形例
光ディスク1101a
コントロールデータ領域
1102
1105a
BCA1104a
ユーザデータ領域1103
トリミング領域1105a
1105a

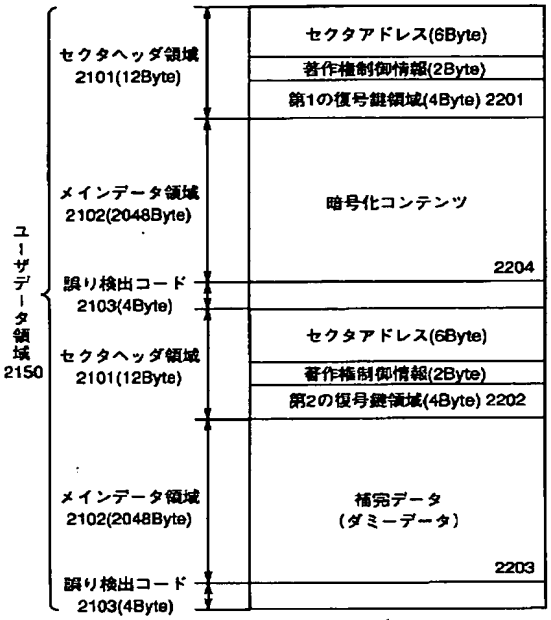
【図２５】


第5の実施形態の変形例
光ディスク1601a
コントロールデータ領域
1602
1606a
BCA1604a
ユーザデータ領域1603
トリミング領域1606a
1606a
記録情報記録領域1605

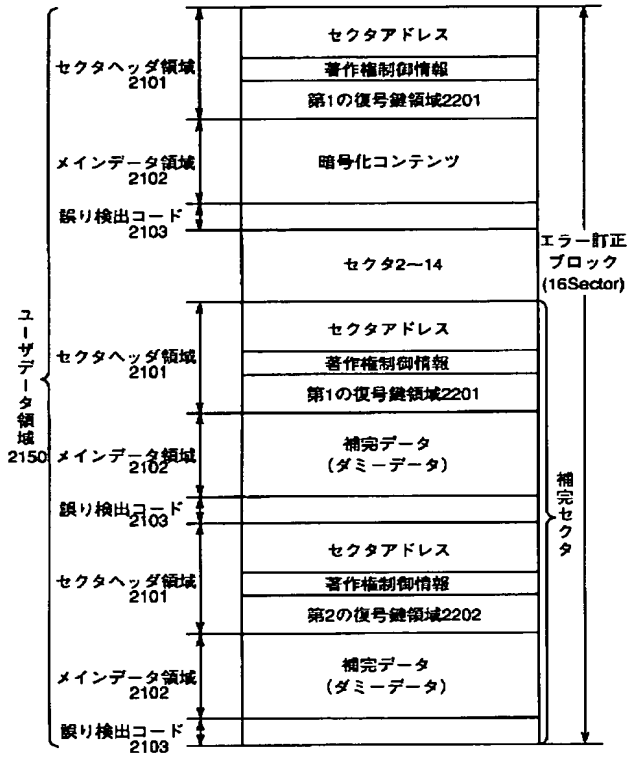
【図２６】


第6の実施形態
光ディスク再生装置
ユーザデータ領域2150
セクタヘッダ領域2101 (12Byte)
メインデータ領域2102 (2048Byte)
誤り検出コード2103 (4Byte)
セクタアドレス(6Byte) 2104
著作権制御情報(2Byte) 2105
復号鍵領域(4Byte) 2106
非暗号化コンテンツ
復号鍵変換データ 2110
暗号化コンテンツ 2108
セクタアドレス(6Byte)
著作権制御情報(2Byte)
復号鍵領域(4Byte) 2109
非暗号化コンテンツ
復号鍵変換データ
暗号化コンテンツ
2111
暗号化復号鍵(8Byte)
データ連結器
2112
ディスク鍵(7Byte)
鍵復号器
パディングデータ(1Byte)+復号鍵(7Byte)
2113
鍵変換器
コンテンツ復号鍵(7Byte)
2114
復号器
復号化コンテンツ

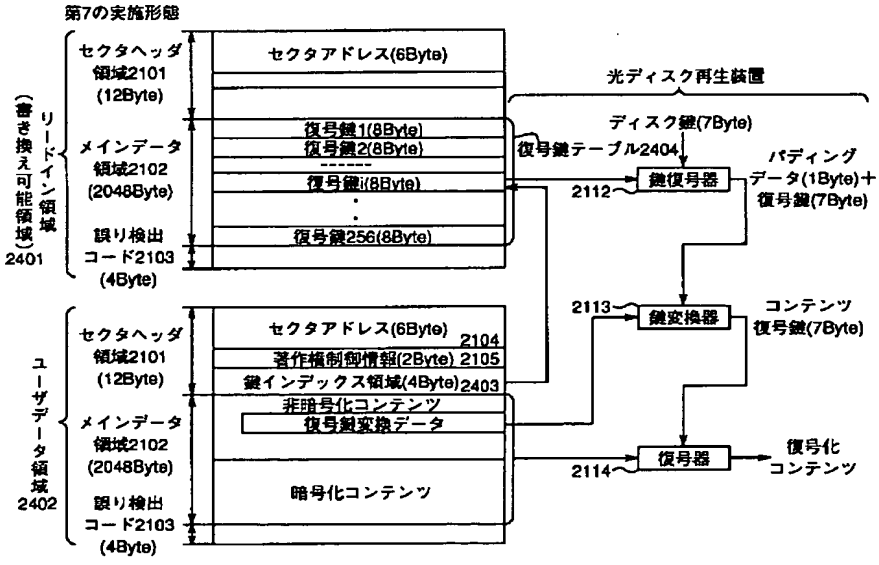
【図２７】


ユーザデータ領域 2150
セクタヘッダ領域 2101(12Byte)
セクタアドレス(6Byte)
著作権制御情報(2Byte)
第1の復号鍵領域(4Byte) 2201
メインデータ領域 2102(2048Byte)
暗号化コンテンツ
2204
誤り検出コード 2103(4Byte)
セクタヘッダ領域 2101(12Byte)
セクタアドレス(6Byte)
著作権制御情報(2Byte)
第2の復号鍵領域(4Byte) 2202
メインデータ領域 2102(2048Byte)
補完データ (ダミーデータ)
2203
誤り検出コード 2103(4Byte)

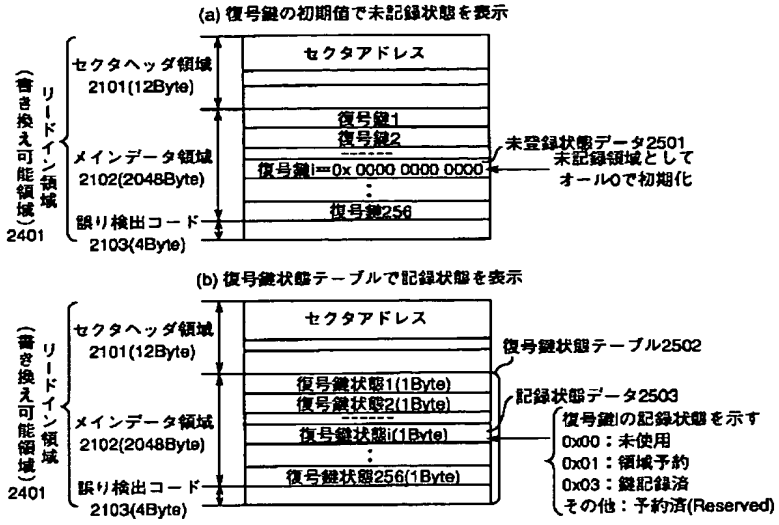
【図２８】


ユーザデータ領域 2150
セクタヘッダ領域 2101
セクタアドレス
著作権制御情報
第1の復号鍵領域2201
メインデータ領域 2102
暗号化コンテンツ
誤り検出コード 2103
セクタ2—14
エラー訂正ブロック (16Sector)
セクタヘッダ領域 2101
セクタアドレス
著作権制御情報
第1の復号鍵領域2201
メインデータ領域 2102
補完データ (ダミーデータ)
誤り検出コード 2103
セクタヘッダ領域 2101
セクタアドレス
著作権制御情報
第2の復号鍵領域2202
メインデータ領域 2102
補完データ (ダミーデータ)
誤り検出コード 2103
補完セクタ

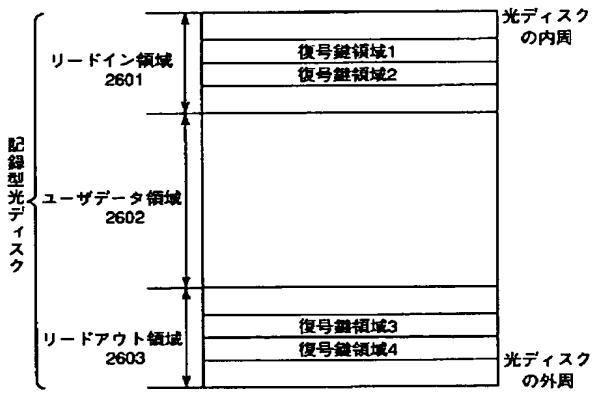
【図２９】


第7の実施形態
リードイン領域 (書き換え可能領域) 2401
セクタヘッダ領域2101 (12Byte)
セクタアドレス(6Byte)
メインデータ領域2102 (2048Byte)
復号鍵1(8Byte)
復号鍵2(8Byte)
復号鍵i(8Byte)
復号鍵256(8Byte)
誤り検出コード2103 (4Byte)
ユーザデータ領域 2402
セクタヘッダ領域2101 (12Byte)
セクタアドレス(6Byte) 2104
著作権制御情報(2Byte) 2105
鍵インデックス領域(4Byte) 2403
メインデータ領域2102 (2048Byte)
非暗号化コンテンツ
復号鍵変換データ
暗号化コンテンツ
誤り検出コード2103 (4Byte)
光ディスク再生装置
ディスク鍵(7Byte)
復号鍵テーブル2404
2112
鍵復号器
パディングデータ(1Byte)+復号鍵(7Byte)
2113
鍵変換器
コンテンツ復号鍵(7Byte)
2114
復号器
復号化コンテンツ

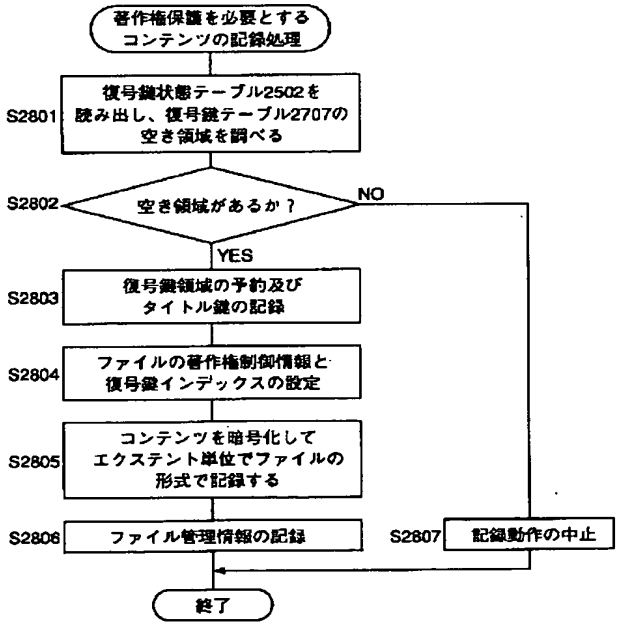
【図３０】



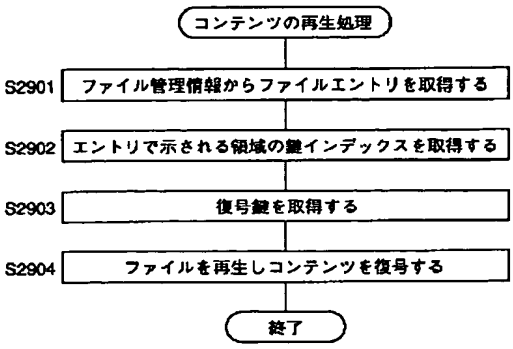
【図３１】



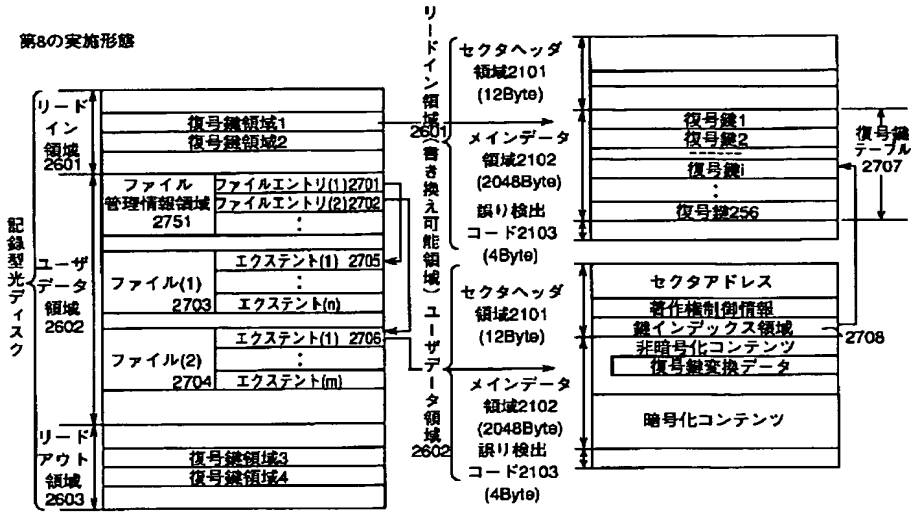
【図３３】



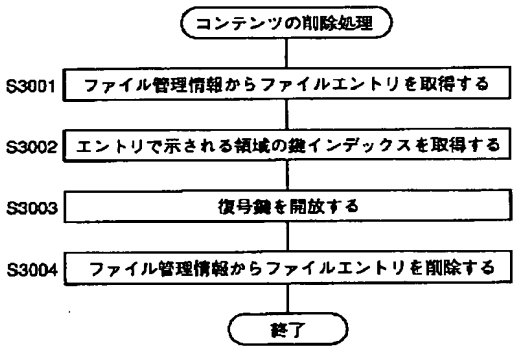
【図３４】



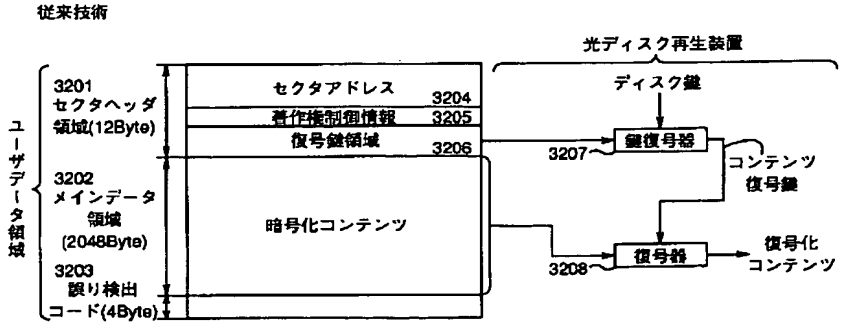
【図３２】


第8の実施形態
記録型光ディスク
リードイン領域2601
ユーザデータ領域2602
リードアウト領域2603
復号鍵領域1
復号鍵領域2
ファイル管理情報領域2751
ファイルエントリ(1)2701
ファイルエントリ(2)2702
ファイル(1)2703
エクステント(1) 2705
エクステント(n)
ファイル(2)2704
エクステント(1) 2706
エクステント(m)
復号鍵領域3
復号鍵領域4
リードイン領域2601（書き換え可能領域）
ユーザデータ領域2602
セクタヘッダ領域2101(12Byte)
メインデータ領域2102(2048Byte)
誤り検出コード2103(4Byte)
復号鍵1
復号鍵2
復号鍵i
復号鍵256
復号鍵テーブル2707
セクタアドレス
著作権制御情報
鍵インデックス領域
非暗号化コンテンツ
復号鍵変換データ
暗号化コンテンツ
2708

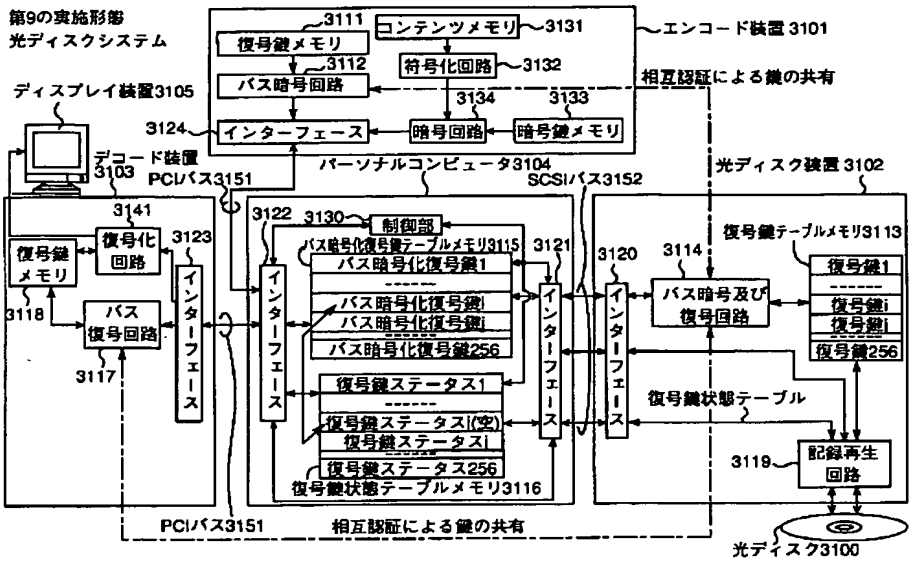
【図３５】


コンテンツの削除処理
S3001
ファイル管理情報からファイルエントリを取得する
S3002
エントリで示される領域の鍵インデックスを取得する
S3003
復号鍵を開放する
S3004
ファイル管理情報からファイルエントリを削除する
終了

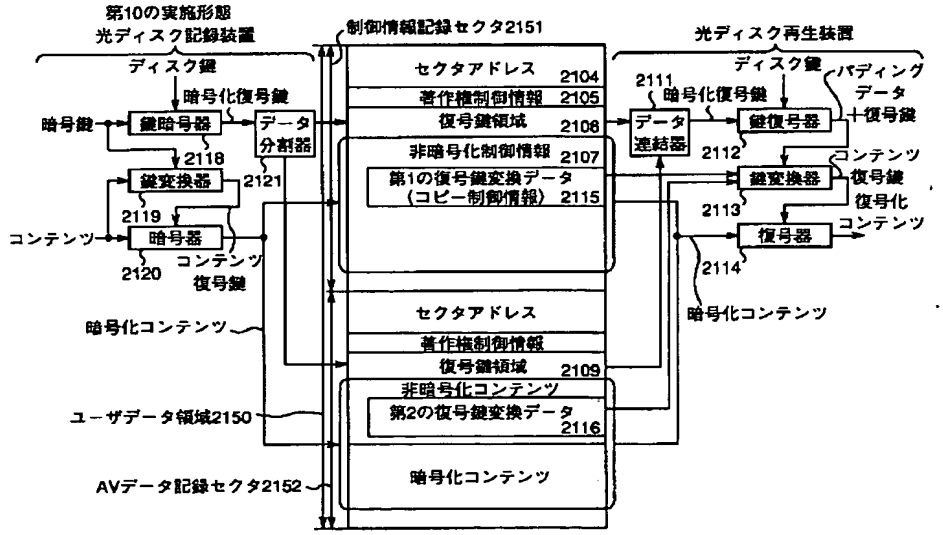
【図３９】


従来技術
光ディスク再生装置
ディスク鍵
ユーザデータ領域
3201 セクタヘッダ領域(12Byte)
3202 メインデータ領域(2048Byte)
3203 誤り検出コード(4Byte)
セクタアドレス
3204
著作権制御情報
3205
復号鍵領域
3206
暗号化コンテンツ
3207
鍵復号器
コンテンツ復号鍵
3208
復号器
復号化コンテンツ

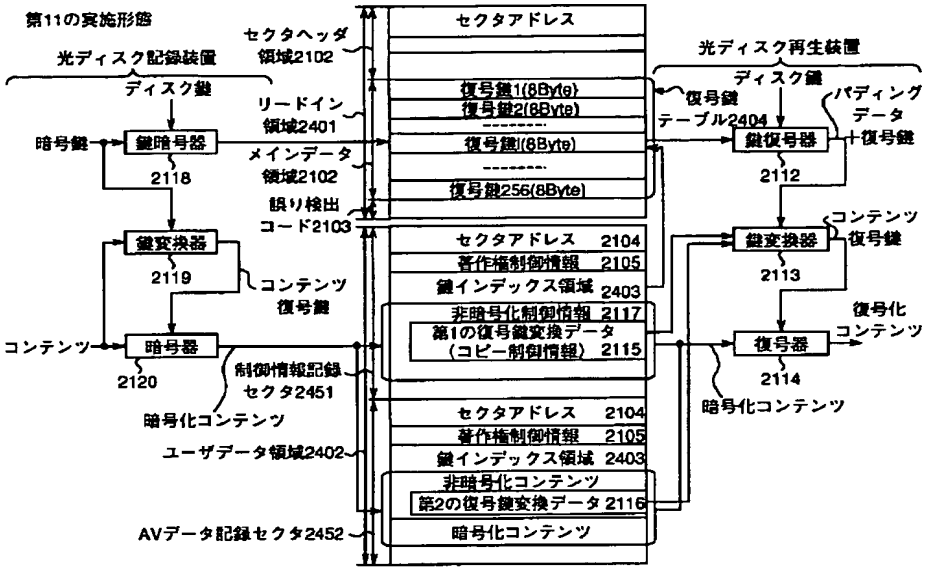
【図３６】


第9の実施形態
光ディスクシステム
ディスプレイ装置3105
デコード装置
3103
PCIバス3151
3141
復号鍵メモリ
復号化回路
3123
3118
バス復号回路
3117
インターフェース
3111
復号鍵メモリ
コンテンツメモリ
3131
3112
パス暗号回路
符号化回路
3132
3134
3133
3124
インターフェース
暗号回路
暗号鍵メモリ
エンコード装置3101
相互認証による鍵の共有
パーソナルコンピュータ3104
SCSIバス3152
光ディスク装置3102
3122
3130
制御部
パス暗号化復号鍵テーブルメモリ3115
パス暗号化復号鍵1
パス暗号化復号鍵i
パス暗号化復号鍵256
3121
復号鍵ステータス1
復号鍵ステータスi(空)
復号鍵ステータスi
復号鍵ステータス256
復号鍵状態テーブルメモリ3116
インターフェース
3120
3114
インターフェース
パス暗号及び復号回路
復号鍵テーブルメモリ3113
復号鍵1
復号鍵i
復号鍵256
復号鍵状態テーブル
3119
記録再生回路
光ディスク3100
PCIバス3151
相互認証による鍵の共有

【図３７】


第10の実施形態
光ディスク記録装置
ディスク鍵
暗号化復号鍵
暗号鍵
鍵暗号器
データ分割器
2118
鍵変換器
2121
2119
暗号器
コンテンツ
2120
コンテンツ復号鍵
暗号化コンテンツ
ユーザデータ領域2150
AVデータ記録セクタ2152
制御情報記録セクタ2151
セクタアドレス
2104
著作権制御情報
2105
復号鍵領域
2106
非暗号化制御情報
2107
第1の復号鍵変換データ
(コピー制御情報)
2115
セクタアドレス
著作権制御情報
復号鍵領域
2109
非暗号化コンテンツ
第2の復号鍵変換データ
2116
暗号化コンテンツ
光ディスク再生装置
ディスク鍵
2111
暗号化復号鍵
パディングデータ
+復号鍵
データ連結器
鍵復号器
2112
コンテンツ
鍵変換器
復号鍵
2113
復号化コンテンツ
復号器
2114
暗号化コンテンツ

【図３８】



フロントページの続き

(51)Int.Cl.[7]		識別記号	FI		テーマコード（参考）
G11B	19/04	501	G11B	19/04	501H
	19/12	501		19/12	501K
	20/10			20/10	H
	20/12			20/12	
H04L	9/08		H04L	9/00	601A
					601E

(72)発明者　高木　裕司
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　弓場　隆司
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　東海林　衛
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　大嶋　光昭
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　大原　俊次
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　伊藤　基志
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　石田　隆
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　中村　敦史
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　謝花　正司
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　中田　浩平
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Ｆターム(参考)　5D029 MA31
5D044 AB05 AB07 BC03 DE22 DE50
GK12 GK17
5D066 DA11 HA01
5D090 AA01 BB02 FF09 GG17 GG24
GG32
5J104 AA01 AA13 AA16 EA17 JA03
NA32 PA14

(54)【発明の名称】　光ディスク、光ディスク記録装置、光ディスク再生装置、光ディスク記録再生装置、光ディスク記録再生方法、光ディスク記録方法、光ディスク再生方法、光ディスク削除方法及び情報処理システム